
Mac OS X Server
Security Configuration
For Version 10.5 Leopard
Second Edition

Apple Inc.
© 2009 Apple Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X software may reproduce this publication for the purpose of learning to use such software. No part of this publication may be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid-for support services.

Every effort has been made to ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Apple
1 Infinite Loop
Cupertino, CA 95014
408-996-1010
www.apple.com

The Apple logo is a trademark of Apple Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AirPort, AppleScript, AppleShare, AppleTalk, Bonjour, Boot Camp, ColorSync, Exposé, FileVault, FireWire, iCal, iChat, iMac, iSight, iTunes, Keychain, Leopard, Mac, Mac Book, Macintosh, Mac OS, QuickTime, Safari, Xgrid, Xsan, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries.

Apple Remote Desktop, Finder, MacBook Air, QuickTime Broadcaster, Spotlight, and Time Machine are trademarks of Apple Inc.

MobileMe is a service mark of Apple Inc., registered in the U.S. and other countries.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Apple is under license.

Intel, Intel Core, and Xeon are trademarks of Intel Corp. in the U.S. and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

PowerPC™ and the PowerPC logo™ are trademarks of International Business Machines Corporation, used under license therefrom.

UNIX is a registered trademark of The Open Group.

X Window System is a trademark of the Massachusetts Institute of Technology

This product includes software developed by the University of California, Berkeley, FreeBSD, Inc., The NetBSD Foundation, Inc., and their respective contributors.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products.

019-1386/2009-10-01

Contents

Preface 18 **About This Guide**
18 Target Audience
18 What's New in Leopard Server
19 What's in This Guide
21 Using This Guide
22 Using Onscreen Help
22 Leopard Server Administration Guides
24 Viewing PDF Guides on Screen
24 Printing PDF Guides
24 Getting Documentation Updates
25 Getting Additional Information
25 Acknowledgments

Chapter 1 26 **Introduction to Leopard Server Security Architecture**
27 Security Architectural Overview
27 UNIX Infrastructure
27 Access Permissions
28 Security Framework
28 Layered Security Defense
29 Credential Management
29 Network Security
29 Public Key Infrastructure (PKI)
30 Authorization Versus Authentication
30 Security Features in Leopard Server
30 Mandatory Access Controls
31 Sandboxing
32 Managed Preferences
32 Quarantine Applications
32 Application-Based Firewall
33 Signed Applications
33 Smart Card Unlock of FileVault and Encrypted Storage
34 Sharing and Collaboration Services
34 Enhanced Encrypted Disk Image Cryptography

35 Enhanced VPN Compatibility and Integration
35 Improved Secure Connectivity

Chapter 2 36 **Installing Leopard Server**
36 System Installation Overview
37 Disabling the Firmware Password
37 Preparing an Administrator Computer
38 The Server Installation Disc
38 Setting Up Network Services
39 Connecting to the Directory During Installation
39 Installing Server Software on a Networked Computer
39 Starting Up for Installation
39 Before Starting Up
40 Remotely Accessing the Install DVD
41 Starting Up from the Install DVD
42 Starting Up from an Alternate Partition
46 Starting Up from a NetBoot Environment
47 Preparing Disks for Installing Leopard Server
54 Identifying Remote Servers When Installing Leopard Server
55 Installing Server Software Interactively
55 Installing Locally from the Installation Disc
57 Installing Remotely with Server Assistant
58 Installing Remotely with VNC
59 Installing Server Software from an Image
59 Using the installer Command-Line Tool to Install Server Software
62 Installing Multiple Servers
63 Upgrading a Computer from Leopard to Leopard Server
63 How to Keep Current
63 Using Interactive Server Setup
66 Setting Up a Local Server Interactively
67 Setting Up a Remote Server Interactively
68 Setting Up Multiple Remote Servers Interactively in a Batch
69 Updating System Software
70 Updating from an Internal Software Update Server
71 Updating from Internet-Based Software Update Servers
71 Updating Manually from Installer Packages
72 Verifying the Integrity of Software
72 Repairing Disk Permissions
73 Kinds of Permissions
73 POSIX Permissions Overview
73 ACL Permissions Overview
74 Using Disk Utility to Repair Disk Permissions

Chapter 3 75 **Protecting System Hardware**
75 Protecting Hardware
76 Preventing Wireless Eavesdropping
76 Understanding Wireless Security Challenges
77 OS Components
77 Removing Wi-Fi Hardware
78 Removing Bluetooth Support Software
79 Removing IR Support Software
80 Preventing Unauthorized Recording
80 Removing Audio Recording Support
81 Removing Video Recording Support Software
82 Preventing Data Port Access
82 Securing USB Hardware
83 Removing FireWire Support Software
84 System Hardware Modifications
84 Authorized AppleCare Certified Technicians

Chapter 4 86 **Securing Global System Settings**
86 Securing System Startup
87 PowerPC-Based Systems
87 Using the Firmware Password Utility
88 Configuring Open Firmware Settings
89 Using Command-Line Tools for Secure Startup
89 Intel-Based Systems
90 Configuring Access Warnings
90 Enabling Access Warnings for the Login Window
91 AuthPlugin Architecture
92 The BannerSample Project
93 Enabling Access Warnings for the Command Line

Chapter 5 94 **Securing Local Server Accounts**
94 Types of User Accounts
95 Guidelines for Securing Accounts
95 Defining User IDs
96 Securing the Guest Account
97 Securing Nonadministrator Accounts
97 Securing Administrator Accounts
98 Securing the Directory Domain Administrator Account
98 Securing the System Administrator Account
99 Restricting sudo Usage
100 Understanding Directory Domains
101 Understanding Network Services, Authentication, and Contacts
102 Configuring LDAPv3 Access

102 Configuring Active Directory Access
103 Using Strong Authentication
103 Using Password Assistant to Generate or Analyze Passwords
104 Using Kerberos
105 Using Smart Cards
105 Using Tokens
106 Using Biometrics
106 Setting Global Password Policies
107 Storing Credentials in Keychains
108 Using the Default User Keychain
108 Creating Additional Keychains
110 Securing Keychains and Their Items
111 Using Smart Cards as Keychains
111 Using Portable and Network Keychains

Chapter 6 112 **Securing System Preferences**
112 System Preferences Overview
114 Securing MobileMe Preferences
116 Securing Accounts Preferences
119 Securing Appearance Preferences
120 Securing Bluetooth Preferences
121 Securing CDs & DVDs Preferences
123 Securing Date & Time Preferences
125 Securing Desktop & Screen Saver Preferences
127 Securing Display Preferences
127 Securing Dock Preferences
128 Securing Energy Saver Preferences
130 Securing Exposé & Spaces Preferences
131 Securing International Preferences
132 Securing Keyboard & Mouse Preferences
132 Securing Network Preferences
133 Disabling Unused Hardware Devices
133 Disabling IPv6
135 Securing Print & Fax Preferences
137 Securing QuickTime Preferences
138 Securing Security Preferences
139 Securing Sharing Preferences
141 Securing Software Update Preferences
142 Securing Sound Preferences
143 Securing Speech Preferences
145 Securing Spotlight Preferences
147 Securing Startup Disk Preferences
149 Securing Time Machine Preferences

150 Securing Universal Access Preferences

Chapter 7 151 **Securing Data and Using Encryption**
151 Permissions
151 Setting POSIX Permissions
152 Viewing POSIX Permissions
153 Interpreting POSIX Permissions
154 Modifying POSIX Permissions
154 Setting File and Folder Flags
154 Viewing Flags
154 Modifying Flags
155 Setting ACL Permissions
156 Enabling ACL Permissions
156 Modifying ACL Permissions
157 Changing Global Umask for Stricter Default Permissions
158 Restricting Setuid Programs
161 Securing User Home Folders
162 Encrypting Home Folders
163 Overview of FileVault
164 Managing FileVault
164 Managing the FileVault Master Keychain
166 Encrypting Portable Files
166 Creating an Encrypted Disk Image
167 Creating an Encrypted Disk Image from Existing Data
168 Creating Encrypted PDFs
169 Securely Erasing Data
169 Configuring Finder to Always Securely Erase
170 Using Disk Utility to Securely Erase a Disk or Partition
170 Using Command-Line Tools to Securely Erase Files
171 Using Secure Empty Trash
171 Using Disk Utility to Securely Erase Free Space
172 Using Command-Line Tools to Securely Erase Free Space

Chapter 8 174 **Securing System Swap and Hibernation Storage**
174 System Swap File Overview
175 Encrypting System Swap

Chapter 9 176 **Avoiding Simultaneous Local Account Access**
176 Fast User Switching
176 Shared User Accounts

Chapter 10 177 **Ensuring Data Integrity with Backups**
177 The Time Machine Architecture
177 Deleting Permanently from Time Machine Backups

178 Storing Backups Inside Secure Storage
178 Restoring Backups from Secure Storage

Chapter 11 179 **Securing Accounts and Share Points**
179 Open Directory and Active Directory
180 Configuring Share Points
180 Disabling Share Points
181 Restricting Access to a Share Point
183 AFP Share Points
183 SMB Share Points
183 FTP Share Points
183 NFS Share Points
185 Controlling Network Views
185 Securing Accounts
185 Configuring User Accounts
187 Configuring Group Accounts
188 Configuring Computer Groups

Chapter 12 189 **Managing Certificates**
189 Understanding Public Key Infrastructure
190 Public and Private Keys
190 Certificates
191 CAs
191 Identities
191 Self-Signed Certificates
191 Obtaining Certificates
192 Using Certificate Manager
193 Requesting a Certificate from a CA
194 Creating a Self-Signed Certificate
194 Importing a Certificate
195 Managing Certificates
195 Editing a Certificate
195 Deleting a Certificate
196 Renewing an Expiring Certificate
196 Creating a CA
196 Creating a CA Using Certificate Assistant
198 Creating a CA from the Command Line
199 Create a Certificate for Someone Else
199 Storing the CA Private Key
199 Creating Folders and Files for SSL
200 Distributing a CA Public Certificate to Clients

Chapter 13 201 **Setting General Protocols and Access to Services**
201 Setting General Protocols
201 Configuring NTP
202 Disabling SNMP
202 Enabling SSH
203 Remote Management (ARD)
203 Restricting Access to Specific Users
204 Remote Apple Events (RAE)
204 Restricting Access to Specific Users
205 Setting the Server's Host Name
205 Setting the Date and Time
205 Setting Up Certificates
205 Setting Service Access Control Lists

Chapter 14 207 **Securing Remote Access Services**
207 Securing Remote Login (SSH)
208 Configuring Secure Shell
209 Modifying the SSH Configuration File
209 Generating Key Pairs for Key-Based SSH Connections
211 Updating SSH Key Fingerprints
212 Controlling Access to SSH
212 SSH Man-in-the-Middle Attacks
213 Transferring Files Using SFTP
213 Securing VPN Service
214 VPN and Security
215 Configuring L2TP/IPSec Settings
216 Configuring PPTP Settings
217 Authentication Method
218 Using VPN Service with Users in a Third-Party LDAP Domain
218 Offering SecurID Authentication with VPN Service
219 Encrypting Observe and Control Network Data
219 Encrypting Network Data During File Copy and Package Installations
220 Remote Apple Events (RAE)
220 Restricting Access to Specific Users

Chapter 15 221 **Securing Network and Host Access Services**
221 Using IPv6 Protocol
222 IPv6-Enabled Services
222 Securing DHCP Service
223 Disabling Unnecessary DHCP Services
223 Configuring DHCP Services
224 Assigning Static IP Addresses Using DHCP
225 Securing DNS Service

226 Understanding BIND
226 Turning Off Zone Transfers
227 Disabling Recursion
227 Understanding DNS Security
228 DNS Cache Poisoning
228 Server Mining
229 DNS Service Profiling
229 Denial of Service (DoS)
230 Service Piggybacking
230 ARP Spoofing
231 Securing Firewall Service
231 Planning Firewall Setup
232 Starting Firewall Service
232 Creating an IP Address Group
233 Creating Firewall Service Rules
234 Creating Advanced Firewall Rules
235 Enabling Stealth Mode
236 Viewing the Firewall Service Log
237 Securing NAT Service
238 Configuring NAT Service
239 Configuring Port Forwarding
240 Securing Bonjour Service

Chapter 16 242 **Securing Collaboration Services**
242 Securing iCal Service
243 Disabling iCal Services
243 Securely Configuring iCal Service
244 Viewing iCal Service Logs
245 Securing iChat Service
245 Disabling iChat Service
245 Securely Configuring iChat Service
249 Viewing iChat Service Logs
249 Securing Wiki Service
249 Disabling Web Service
250 Securely Configuring Wiki Services
250 Viewing Wiki Service Logs
250 Securing Podcast Producer Service
251 Disabling Podcast Producer Service
251 Securely Configuring Podcast Producer Service
252 Viewing Podcast Producer Service Logs

Chapter 17 253 **Securing Mail Service**
253 Disabling Mail Service

254 Configuring Mail Service for SSL
255 Enabling Secure Mail Transport with SSL
255 Enabling Secure POP Authentication
256 Configuring SSL Transport for POP Connections
256 Enabling Secure IMAP Authentication
257 Configuring SSL Transport for IMAP Connections
258 Enabling Secure SMTP Authentication
259 Configuring SSL Transport for SMTP Connections
260 Using ACLs for Mail Service Access
261 Limiting Junk Mail and Viruses
261 Connection Control
265 Filtering SMTP Connections
265 Mail Screening
270 Viewing Mail Service Logs

Chapter 18 271 **Securing Antivirus Services**
272 Securely Configuring and Managing Antivirus Services
272 Enabling Virus Scanning
273 Managing ClamAV with ClamXav
273 Viewing Antivirus Services Logs

Chapter 19 274 **Securing File Services**
274 Security Considerations
274 Restricting Access to File Services
274 Restricting Access to Everyone
275 Restricting Access to NFS Share Points
275 Restricting Guest Access
275 Restricting File Permissions
276 Protocol Security Comparison
276 Disabling File Services
277 Choosing a File Sharing Protocol
278 Configuring AFP File Sharing Service
280 Configuring FTP File Sharing Service
282 Configuring NFS File Sharing Service
283 Configuring SMB File Sharing Service

Chapter 20 285 **Securing Web Service**
285 Disabling Web Service
286 Managing Web Modules
287 Disabling Web Options
288 Using Realms to Control Access
290 Enabling Secure Sockets Layer (SSL)
292 Using a Passphrase with SSL Certificates

292 Viewing Web Service Logs
293 Securing WebDAV
294 Securing Blog Services
294 Disabling Blog Services
295 Securely Configuring Blog Services
296 Viewing Blog Service Logs
296 Securing Tomcat
296 Securing MySQL
296 Disabling MySQL Service
297 Setting Up MySQL Service
298 Viewing MySQL Service and Admin Logs
298 Securing WebObjects

Chapter 21 300 **Securing Client Configuration Management Services**
300 Managing Applications Preferences
301 Controlling User Access to Applications and Folders
303 Allowing Specific Dashboard Widgets
304 Disabling Front Row
305 Allowing Legacy Users to Open Applications and Folders
306 Managing Dock Preferences
307 Managing Energy Saver Preferences
308 Managing Finder Preferences
310 Managing Login Preferences
313 Managing Media Access Preferences
314 Managing Mobility Preferences
316 Managing Network Preferences
317 Managing Parental Controls Preferences
318 Hiding Profanity in Dictionary
318 Preventing Access to Adult Websites
319 Allowing Access Only to Specific Websites
320 Setting Time Limits and Curfews on Computer Usage
321 Managing Printing Preferences
322 Managing Software Update Preferences
323 Managing Access to System Preferences
324 Managing Universal Access Preferences
325 Enforcing Policy

Chapter 22 326 **Securing NetBoot Service**
326 Securing NetBoot Service
326 Disabling NetBoot Service
327 Securely Configuring NetBoot Service
328 Viewing NetBoot Service Logs

Chapter 23 330 **Securing Software Update Service**
330 Disabling Software Update Service
331 Securely Configuring Software Update Service
332 Viewing Software Update Service Logs

Chapter 24 333 **Securing Directory Services**
334 Open Directory Server Roles
334 Configuring the Open Directory Services Role
335 Starting Kerberos After Setting Up an Open Directory Master
337 Configuring Open Directory for SSL
338 Configuring Open Directory Policies
339 Setting the Global Password Policy
340 Setting a Binding Policy for an Open Directory Master and Replicas
341 Setting a Security Policy for an Open Directory Master and Replicas

Chapter 25 343 **Securing RADIUS Service**
343 Disabling RADIUS Service
344 Securely Configuring RADIUS Service
344 Configuring RADIUS to Use Certificates
345 Editing RADIUS Access
346 Viewing RADIUS Service Logs

Chapter 26 347 **Securing Print Service**
347 Disabling Print Service
348 Securing Print Service
348 Configuring Print Service Access Control Lists
349 Configuring Kerberos
350 Configuring Print Queues
351 Viewing Print Service and Queue Logs

Chapter 27 353 **Securing Multimedia Services**
353 Disabling QTSS
354 Securely Configuring QTSS
355 Configuring a Streaming Server
355 Serving Streams Through Firewalls Using Port 80
356 Streaming Through Firewalls or Networks with Address Translation
357 Changing the Password Required to Send an MP3 Broadcast Stream
357 Using Automatic Unicast (Announce) with QTSS on a Separate Computer
357 Controlling Access to Streamed Media
361 Viewing QTSS Logs

Chapter 28 363 **Securing Grid and Cluster Computing Services**
363 Understanding Xgrid Service
364 Disabling Xgrid Service

364 Authentication Methods for Xgrid
365 Single Sign-On
366 Password-Based Authentication
366 No Authentication
366 Securely Configuring Xgrid Service
366 Configuring an Xgrid Agent
368 Configuring an Xgrid Controller

Chapter 29 369 **Managing Who Can Obtain Administrative Privileges (sudo)**
369 Managing the sudoers File

Chapter 30 371 **Managing Authorization Through Rights**
371 Understanding the Policy Database
371 The Rights Dictionary
373 Rules
374 Managing Authorization Rights
374 Creating an Authorization Right
374 Modifying an Authorization Right
374 Example Authorization Restrictions

Chapter 31 376 **Maintaining System Integrity**
376 Using Digital Signatures to Validate Applications and Processes
377 Validating Application Bundle Integrity
378 Validating Running Processes
378 Auditing System Activity
378 Installing Auditing Tools
379 Enabling Auditing
380 Setting Audit Mechanisms
380 Using Auditing Tools
380 Using the audit Tool
381 Using the auditreduce Tool
382 Using the praudit Tool
383 Deleting Audit Records
383 Audit Control Files
384 Managing and Analyzing Audit Log Files
384 Using Activity Analysis Tools
385 Validating System Logging
385 Configuring syslogd
386 Local System Logging
386 Remote System Logging
387 Viewing Logs in Server Admin

Chapter 32 388 **Configuring the IPFW2 Firewall**
388 Firewall Protection

388 The IPFW2 Firewall
389 Configuring the IPFW Firewall
389 Understanding IPFW Rulesets
390 Implementing an IPFW Ruleset

Appendix A 394 **Understanding Passwords and Authentication**
394 Password Types
394 Authentication and Authorization
395 Open Directory Passwords
396 Shadow Passwords
396 Crypt Passwords
396 Offline Attacks on Passwords
397 Password Guidelines
397 Creating Complex Passwords
397 Using an Algorithm to Create a Complex Password
398 Safely Storing Your Password
399 Password Maintenance
399 Authentication Services
400 Determining Which Authentication Option to Use
401 Password Policies
401 Single Sign-On Authentication
402 Kerberos Authentication
403 Smart Card Authentication

Appendix B 404 **Security Checklist**
404 Installation Action Items
405 Hardware and Core Leopard Server Action Items
405 Global Settings for Leopard Server Action Items
406 Account Configuration Action Items
406 System Software Action Items
407 MobileMe Preferences Action Items
407 Accounts Preferences Action Items
407 Appearance Preferences Action Items
408 Bluetooth Preferences Action Items
408 CDs & DVDs Preferences Actions Items
408 Exposé & Spaces Preferences Action Items
408 Date & Time Preferences Action Items
409 Desktop & Screen Saver Preferences Action Items
409 Display Preferences Action Items
409 Dock Preferences Action Items
409 Energy Saver Preferences Action Items
410 Keyboard and Mouse Preferences Action Items
410 Network Preferences Action Items

410 Print & Fax Preferences Action Items
410 QuickTime Preferences Action Items
411 Security Preferences Action Items
411 Sharing Preferences Action Items
411 Software Update Preferences Action Items
411 Sound Preferences Action Items
412 Speech Preferences Action Items
412 Spotlight Preferences Action Items
412 Startup Disk Preferences Action Items
412 Time Machine Preferences Action Items
412 Data Maintenance and Encryption Action Items
413 Account Policies Action Items
413 Share Points Action Items
413 Account Configuration Action Items
414 Applications Preferences Action Items
414 Dock Preferences Action Items
415 Energy Saver Preferences Action Items
415 Finder Preferences Action Items
415 Login Preferences Action Items
416 Media Access Preferences Action Items
417 Mobility Preferences Action Items
417 Network Preferences Action Items
417 Printing Preferences Action Items
418 Software Update Preferences Action Items
418 Access to System Preferences Action Items
418 Universal Access Preferences Action Items
419 Certificates Action Items
419 General Protocols and Service Access Action Items
420 Remote Access Services Action Items
420 Network and Host Access Services Action Items
421 IPv6 Protocol Action Items
421 DHCP Service Action Items
421 DNS Service Action Items
422 Firewall Service Action Items
422 NAT Service Action Items
422 Bonjour Service Action Items
422 Collaboration Services Action Items
423 Mail Service Action Items
424 File Services Action Items
424 AFP File Sharing Service Action Items
424 FTP File Sharing Service Action Items
425 NFS File Sharing Service Action Items
425 SMB Action Items

426 Web Service Action Items
426 Client Configuration Management Services Action Items
426 Directory Services Action Items
427 Print Service Action Items
427 Multimedia Services Action Items
427 Grid and Cluster Computing Services Action Items
428 Validating System Integrity Action Items

Appendix C 429 **Scripts**

Glossary 469

Index 481

About This Guide

Use this guide as an overview of Leopard Server security features that can enhance security on your computer.

This guide gives instructions for securing Leopard Server or later, and for securely managing servers and clients in a networked environment. It also provides information about the many roles Leopard Server can assume in a network.

Target Audience

Administrators of server computers running Leopard Server or later are the intended audience for this guide.

If you're using this guide, you should be an experienced Leopard Server user, be familiar with the Workgroup Manager and Server Admin applications, and have at least some experience using the Terminal application's command-line interface.

You should also have experience administering a network, be familiar with basic networking concepts, and be familiar with the Leopard Server administration guides.

Some instructions in this guide are complex, and deviation from them could result in serious adverse effects on the server and its security. These instructions should only be used by experienced Leopard Server administrators, and should be followed by thorough testing.

What's New in Leopard Server

Server Leopard offers major security enhancements in the following key areas:

- **Better Trojan horse protection.** Leopard Server marks files that are downloaded to help prevent users from inadvertently running malicious downloaded applications.
- **Stronger runtime security.** New technologies such as library randomization and sandboxing help prevent attacks that try to hijack or modify the software on your system.

- **Easier network security.** After you've activated the new Leopard Server application firewall, it configures itself so you get the benefits of firewall protection without needing to understand the details of network ports and protocols.
- **Improved secure connectivity.** Virtual private network (VPN) support has been enhanced to connect to more of the most popular VPN servers—without additional software.
- **Meaningful security alerts.** When users receive security alerts and questions too frequently, they can fall into reflexive mode when the system asks a security-related question, clicking OK without thought. Leopard Server is designed to minimize the number of security alerts that you see, so when you do see one, it gets your attention.

What's in This Guide

This guide explains how to secure servers and securely manage server and client computers in a networked environment. It does not provide information about securing clients. For help with securing computers running Mac OS X v10.5 Leopard or later, see *Mac OS X Security Configuration*.

This guide cannot cover all possible network configurations in which Leopard Server might be used. Good network security and design must be used for this information to be effective, and anyone using this guide needs to be familiar with UNIX security basics, such as setting file permissions.

This guide includes the following chapters, arranged in the order that you're likely to need them when securely configuring a server.

- Chapter 1, "Introduction to Leopard Server Security Architecture," provides an overview of the security architecture and features of Leopard Server. This chapter describes the security framework, access permissions, built-in security services, and directory services.
- Chapter 2, "Installing Leopard Server," describes how to securely install Leopard Server locally or remotely. This chapter also includes information about updating system software, repairing disk permissions, and securely erasing data.
- Chapter 3, "Protecting System Hardware," describes how to physically protect your hardware from attacks.
- Chapter 4, "Securing Global System Settings," describes how to secure settings that affect all users of the computer.
- Chapter 5, "Securing Local Server Accounts," describes the types of user accounts and how to securely configure an account. This includes securing accounts using strong authentication.

- Chapter 6, "Securing System Preferences," helps you configure your local server accounts securely. This includes the secure configuration of local system preferences, setting up strong authentication and credential storage, and securing data.
- Chapter 7, "Securing Data and Using Encryption," describes how to encrypt data and how to use secure erase to ensure old data is completely removed.
- Chapter 8, "Securing System Swap and Hibernation Storage," describes how to scrub your system swap and hibernation space of sensitive information.
- Chapter 9, "Avoiding Simultaneous Local Account Access," describes how to protect your data from the security vulnerabilities of multiple users using single accounts.
- Chapter 10, "Ensuring Data Integrity with Backups," describes the Time Machine architecture and how to securely back up and restore your computer and data.
- Chapter 11, "Securing Accounts and Share Points," describes security settings related to managed user and group accounts.
- Chapter 12, "Managing Certificates," describes how to generate, request, and deploy certificates.
- Chapter 13, "Setting General Protocols and Access to Services," helps you configure general network management protocols and restrict access to other services.
- Chapter 14, "Securing Remote Access Services," tells you how to create remote connections to your server using encryption.
- Chapter 15, "Securing Network and Host Access Services," explains how to connect client computers and configure a firewall.
- Chapter 16, "Securing Collaboration Services," describes how to securely configure iChat, iCal, Wiki, and Podcast Producer services.
- Chapter 17, "Securing Mail Service," explains how to set up mail service to use encryption and filter for spam and viruses.
- Chapter 18, "Securing Antivirus Services," describes how to enable and manage antivirus services to protect your mail and files.
- Chapter 19, "Securing File Services," explains how to configure file services to enable secure data sharing.
- Chapter 20, "Securing Web Service," describes how to set up a web server and secure web settings and components.
- Chapter 21, "Securing Client Configuration Management Services," helps you set policies and enforce them using Workgroup Manager.
- Chapter 22, "Securing NetBoot Service," tells you how to configure NetBoot securely to provide images to clients.
- Chapter 23, "Securing Software Update Service," describes how to securely configure software update services.
- Chapter 24, "Securing Directory Services," explains how to configure Open Directory service roles and password policies.

- Chapter 25, "Securing RADIUS Service," tells how to securely configure the RADIUS service.
- Chapter 26, "Securing Print Service," explains how to set up print queues and banner pages.
- Chapter 27, "Securing Multimedia Services," provides security information to configure a streaming server.
- Chapter 28, "Securing Grid and Cluster Computing Services," explains how to securely configure an Xgrid agent and controller.
- Chapter 29, "Managing Who Can Obtain Administrative Privileges (sudo)," describes how to restrict access to the `sudo` command.
- Chapter 30, "Managing Authorization Through Rights," explains the policy database and how to control authorization by managing rights in the policy database.
- Chapter 31, "Maintaining System Integrity," describes how to use security audits and logging to validate the integrity of your server and data.
- Chapter 32, "Configuring the IPFW2 Firewall," describes how to configure the IPFW2 firewall.
- Appendix A, "Understanding Passwords and Authentication," describes Open Directory authentication, shadow and crypt passwords, Kerberos, LDAP bind, and single sign-on.
- Appendix B, "Security Checklist," provides a checklist that guides you through securing your server.
- Appendix C, "Scripts," provides command-line commands and scripts for securing your server.

In addition, the Glossary defines terms you'll encounter as you read this guide.

Note: Because Apple frequently releases new versions and updates to its software, images shown in this book might be different from what you see on your screen.

Using This Guide

The following list contains suggestions for using this guide:

- Read the guide in its entirety. Subsequent sections might build on information and recommendations discussed in prior sections.
- The instructions in this guide should always be tested in a nonoperational environment before deployment. This nonoperational environment should simulate, as much as possible, the environment where the computer will be deployed.
- This information is intended for computers running Leopard Server. Before securely configuring a server, determine what function that particular server will perform and apply security configurations where applicable.

- Use the security checklist in Appendix B to track and record each security task and note what settings you changed. This information can be helpful when developing a security standard within your organization.

Important: Any deviation from this guide should be evaluated to determine what security risks it might introduce. Take measures to monitor or mitigate those risks.

Using Onscreen Help

You can get task instructions onscreen in Help Viewer while you're managing Leopard Server. You can view help on a server or an administrator computer. (An administrator computer is a computer running Leopard Server)

To get help for an advanced configuration of Leopard Server:

- Open Server Admin or Workgroup Manager and then:
 - Use the Help menu to search for a task you want to perform.
 - Choose Help > Server Admin Help or Help > Workgroup Manager Help to browse and search the help topics.

The onscreen help contains instructions taken from *Server Administration* and other advanced administration guides described in "Leopard Server Administration Guides," next.

To see the most recent server help topics:

- Make sure the server or administrator computer is connected to the Internet while you're getting help.

 Help Viewer automatically retrieves and caches the most recent server help topics from the Internet. When not connected to the Internet, Help Viewer displays cached help topics.

Leopard Server Administration Guides

Getting Started covers installation and setup for standard and workgroup configurations of Mac OS X Server. For advanced configurations, *Server Administration* covers planning, installation, setup, and general server administration. A suite of additional guides, listed below, covers advanced planning, setup, and management of individual services. You can get these guides in PDF format from the Mac OS X Server documentation website:

www.apple.com/server/documentation.

This guide…	tells you how to:
Getting Started and *Installation & Setup Worksheet*	Install Leopard Server and set it up for the first time.
Command-Line Administration	Install, set up, and manage Leopard Server using UNIX command-line tools and configuration files.
File Services Administration	Share selected server volumes or folders among server clients using the AFP, NFS, FTP, and SMB protocols.
iCal Service Administration	Set up and manage iCal shared calendar service.
iChat Service Administration	Set up and manage iChat instant messaging service.
Mac OS X Security Configuration	Make Mac OS X computers (clients) more secure, as required by enterprise and government customers.
Mac OS X Server Security Configuration	Make Mac OS X Server and the computer it's installed on more secure, as required by enterprise and government customers.
Mail Service Administration	Set up and manage IMAP, POP, and SMTP mail services on the server.
Network Services Administration	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, NAT, and RADIUS services on the server.
Open Directory Administration	Set up and manage directory and authentication services, and configure clients to access directory services.
Podcast Producer Administration	Set up and manage Podcast Producer service to record, process, and distribute podcasts.
Print Service Administration	Host shared printers and manage their associated queues and print jobs.
QuickTime Streaming and Broadcasting Administration	Capture and encode QuickTime content. Set up and manage QuickTime streaming service to deliver media streams live or on demand.
Server Administration	Perform advanced installation and setup of server software, and manage options that apply to multiple services or to the server as a whole.
System Imaging and Software Update Administration	Use NetBoot, NetInstall, and Software Update to automate the management of operating system and other software used by client computers.
Upgrading and Migrating	Use data and service settings from an earlier version of Mac OS X Server or Windows NT.
User Management	Create and manage user accounts, groups, and computers. Set up managed preferences for Mac OS X clients.
Web Technologies Administration	Set up and manage web technologies, including web, blog, webmail, wiki, MySQL, PHP, Ruby on Rails, and WebDAV.
Xgrid Administration and High Performance Computing	Set up and manage computational clusters of Xserve systems and Mac computers.
Mac OS X Server Glossary	Learn about terms used for server and storage products.

Viewing PDF Guides on Screen

While reading the PDF version of a guide onscreen:

- Show bookmarks to see the guide's outline, and click a bookmark to jump to the corresponding section.
- Search for a word or phrase to see a list of places where it appears in the document. Click a listed place to see the page where it occurs.
- Click a cross-reference to jump to the referenced section. Click a web link to visit the website in your browser.

Printing PDF Guides

If you want to print a guide, you can take these steps to save paper and ink:

- Save ink or toner by not printing the cover page.
- Save color ink on a color printer by looking in the panes of the Print dialog for an option to print in grays or black and white.
- Reduce the bulk of the printed document and save paper by printing more than one page per sheet of paper. In the Print dialog, change Scale to 115% (155% for *Getting Started*). Then choose Layout from the untitled pop-up menu. If your printer supports two-sided (duplex) printing, select one of the Two-Sided options. Otherwise, choose 2 from the Pages per Sheet pop-up menu, and optionally choose Single Hairline from the Border menu. (If you're using Mac OS X v10.4 Tiger or earlier, the Scale setting is in the Page Setup dialog and the Layout settings are in the Print dialog.)

You may want to enlarge the printed pages even if you don't print double sided, because the PDF page size is smaller than standard printer paper. In the Print dialog or Page Setup dialog, try changing Scale to 115% (155% for *Getting Started*, which has CD-size pages).

Getting Documentation Updates

Periodically, Apple posts revised help pages and new editions of guides. Some revised help pages update the latest editions of the guides.

- To view new onscreen help topics for a server application, make sure your server or administrator computer is connected to the Internet and click "Latest help topics" or "Staying current" in the main help page for the application.
- To download the latest guides in PDF format, go to the Mac OS X Server documentation website:

 www.apple.com/server/documentation
- An RSS feed listing the latest updates to Mac OS X Server documentation and onscreen help is available. To view the feed use an RSS reader application, such as Safari or Mail:

 feed://helposx.apple.com/rss/leopard/serverdocupdates.xml

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx)—gateway to extensive product and technology information.
- *Mac OS X Server Support website* (www.apple.com/support/macosxserver)—access to hundreds of articles from Apple's support organization.
- *Apple Training website* (www.apple.com/training)—instructor-led and self-paced courses for honing your server administration skills.
- *Apple Discussions website* (discussions.apple.com)—a way to share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Product Security Mailing Lists website* (lists.apple.com/mailman/listinfo/security-announce/)—Mailing lists for communicating by email with other administrators about security notifications and announcements.
- *Open Source website* (developer.apple.com/darwin/)—Access to Darwin open source code, developer information, and FAQs.
- *Apple Product Security website* (www.apple.com/support/security/)—Access to security information and resources, including security updates and notifications.

For additional security-specific information, consult these resources:

- *NSA security configuration guides* (www.nsa.gov/snac/)—The National Security Agency (NSA) provides information about securely configuring proprietary and open source software.
- *NIST Security Configuration Checklists Repository* (checklists.nist.gov/repository/category.html)—This is the National Institute of Standards and Technology (NIST) repository for security configuration checklists.
- *DISA Security Technical Implementation Guide* (www.disa.mil/gs/dsn/policies.html)—This is the Defense Information Systems Agency (DISA) guide for implementing secure government networks. A Department of Defense (DoD) PKI Certificate is required to access this information.
- *CIS Benchmark and Scoring Tool* (www.cisecurity.org/bench_osx.html)—This is the Center for Internet Security (CIS) benchmark and scoring tool used to establish CIS benchmarks.

Acknowledgments

Apple would like to thank the NSA, NIST, and DISA for their assistance in creating and editing the security configuration guides for Leopard and Leopard Server.

Introduction to Leopard Server Security Architecture

1

Use this chapter to learn about the features in Leopard Server that can enhance security on your computer

Security has never been a more important consideration when selecting a computer platform. Whether you're a home user with a broadband Internet connection, a professional with a mobile computer, or an IT manager with thousands of networked systems, you need to safeguard the confidentiality of information and the integrity of your computers.

With Leopard Server, a security strategy is implemented that is central to the design of the operating system are designed to enhance security on your computer, Leopard Server provides the following features.

- **Modern security architecture.** Leopard includes state-of-the-art, standards-based technologies that enable Apple and third-party developers to build secure software for the Mac. These technologies support all aspects of system, data, and networking security required by today's applications.
- **Secure default settings.** When you take your Mac out of the box, it is securely configured to meet the needs of most common environments, so you don't need to be a security expert to set up your computer. The default settings are designed to make it very difficult for malicious software to infect your computer. You can further configure security on the computer to meet organizational or user requirements.
- **Innovative security applications.** Leopard includes features that take the worry out of using a computer. For example, FileVault protects your documents by using strong encryption, an integrated VPN client gives you secure access to networks over the Internet, and a powerful firewall secures your home network.
- **Open source foundation.** Open source methodology makes Leopard a robust, secure operating system, because its core components have been subjected to peer review for decades. Problems can be quickly identified and fixed by Apple and the larger open source community.

- **Rapid response.** Because the security of your computer is important, Apple responds rapidly to provide patches and updates. Apple works with worldwide partners, including the Computer Emergency Response Team (CERT), to notify users of potential threats. If vulnerabilities are discovered, the built-in Software Update tool notifies users of security updates, which are available for easy retrieval and installation.

Security Architectural Overview

Leopard Server security services are built on two open source standards:

- **Berkeley Software Distribution (BSD).** BSD is a form of UNIX that provides fundamental services, including the Leopard Server file system and file access permissions.
- **Common Data Security Architecture (CDSA).** CDSA provides a wide array of security services, including more specific access permissions, authentication of user identities, encryption, and secure data storage.

UNIX Infrastructure

The Leopard Server kernel—the heart of the operating system—is built from BSD and Mach.

Among other things, BSD provides basic file system and networking services and implements a user and group identification scheme. BSD enforces access restrictions to files and system resources based on user and group IDs.

Mach provides memory management, thread control, hardware abstraction, and interprocess communication. Mach enforces access by controlling which tasks can send a message to a Mach port. (A Mach port represents a task or some other resource.) BSD security policies and Mach access permissions constitute an essential part of security in Leopard Server, and are both critical to enforcing local security.

Access Permissions

An important aspect of computer security is the granting or denying of access permissions (sometimes called access rights). A permission is the ability to perform a specific operation, such as gaining access to data or to execute code.

Permissions are granted at the level of folders, subfolders, files, or applications. Permissions are also granted for specific data in files or for application functions.

Permissions in Leopard Server are controlled at many levels, from the Mach and BSD components of the kernel through higher levels of the operating system, and—for networked applications—through network protocols.

Security Framework

The security framework in Leopard is an implementation of the CDSA architecture. It contains an expandable set of cryptographic algorithms to perform code signing and encryption operations while maintaining the security of the cryptographic keys. It also contains libraries that allow the interpretation of X.509 certificates.

The CDSA code is used by Leopard features such as Keychain and URL Access for protection of login data.

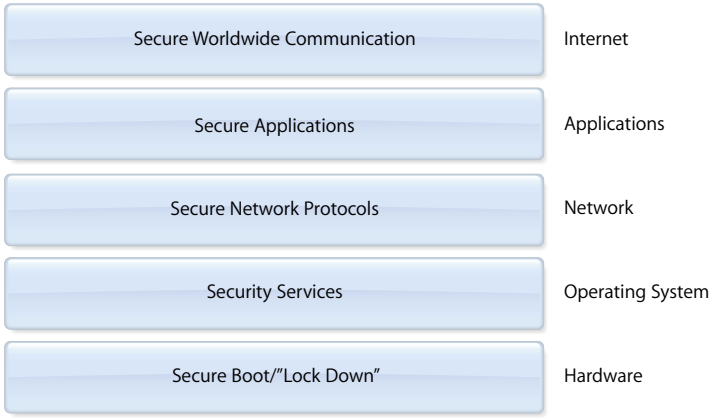
Apple built the foundation of Leopard and many of its integrated services with open source software—such as FreeBSD, Apache, and Kerberos, among others—that has been made secure through years of public scrutiny by developers and security experts around the world.

Strong security is a benefit of open source software because anyone can inspect the source code, identify theoretical vulnerabilities, and take steps to strengthen the software.

Apple actively participates with the open source community by routinely releasing updates of Leopard Server that are subject to independent developers' ongoing review—and by incorporating improvements. An open source software development approach provides the transparency necessary to ensure that Leopard Server is truly secure.

Layered Security Defense

Leopard Server security is built on a layered defense for maximum protection. Security features such as the following provide solutions for securing data at all levels, from the operating system and applications to networks and the Internet.



- Secure worldwide communication—Firewall and mail filtering help prevent malicious software from compromising your computer.

- Secure applications—FileVault (an application of encrypted disk images) helps prevent intruders from using your applications and viewing data on your computer.
- Secure network protocols—Secure Sockets Layer (SSL) is a protocol that helps prevent intruders from viewing information exchange across a network, and Kerberos secures the authentication process.
- Security Services—Authentication using keychains, together with POSIX and ACL permissions, helps prevent intruders from using your applications and accessing your files.
- Secure hardware—The Firmware Password Utility helps prevent people who can access your hardware from gaining root-level access permissions to your computer files.

Credential Management

A keychain is used to store passwords, keys, certificates, and other data placed in the keychain by a user. Due to the sensitive nature of this information, keychains use cryptography to encrypt and decrypt secrets, and they safely store secrets and related data in files.

Leopard Server Keychain services enable you to create keychains and securely store keychain items. After a keychain is created, you can add, delete, and edit keychain items, such as passwords, keys, certificates, and notes for users.

A user can unlock a keychain through authentication (by using a password, digital token, smart card) and applications can then use that keychain to store and retrieve data, such as passwords.

Network Security

The default security settings on your Leopard Server computer are configured to be secure from local network and Internet attacks.

Secure Transport is used to implement SSL and Transport Layer Security (TLS) protocols. These protocols provide secure communications over a TCP/IP connection such as the Internet by using encryption and certificate exchange.

Public Key Infrastructure (PKI)

Certificate, key, and trust services include functions to:

- Create, manage, and read certificates
- Add certificates to a keychain
- Create encryption keys
- Manage trust policies

These functions are used when the services call Common Security Service Manager (CSSM) functions. This is transparent to users.

Authorization Versus Authentication

Authorization is the process by which an entity, such as a user or a computer, demonstrates that they are who they say they are and as a result obtains the right to perform a restricted operation.

For example, the user, entering a password which only he or she could know, allows the system to authenticate that user.

Authorization can also refer to the right itself, as in "Anne has the authorization to run that program." Authorization usually involves authenticating the entity and then determining whether it has the correct permissions.

Authentication is normally done as a step in the authorization process. Some applications and operating system components carry out their own authentication. Authentication might use authorization services when necessary.

Security Features in Leopard Server

Leopard Server includes the following new security features and technologies to enhance the protection of your computer and your personal information.

- **Tagging and first-run warning**: Leopard Server marks files that are downloaded to help prevent users from inadvertently running malicious downloaded applications.
- **Runtime Protection:** New technologies such as execute disable, library randomization, and sandboxing help prevent attacks that try to hijack or modify the software on your system.
- **Improved Firewall**: After you activate the new application firewall, the firewall configures itself to restrict incoming applications for users without requiring the user to write complicated rules.
- **Mandatory access control**: These enforce restrictions on access to system resources.
- **Application signing**: This enables you to verify the integrity and identity of applications on your Mac.

Mandatory Access Controls

Leopard Server introduces a new access control mechanism known as mandatory access controls. Although the Mandatory Access Control technology is not visible to users, it is included in Leopard Server to protect your computer.

Mandatory access controls are policies that cannot be overridden. These policies set security restrictions created by the developer. This approach is different from discretionary access controls that permit users to override security policies according to their preferences.

Mandatory access controls in Leopard Server aren't directly visible to users, but they are the underlying technology that helps enable several important new features, including sandboxing, parental controls, managed preferences, and a safety net feature for Time Machine.

The Time Machine feature illustrates the difference between mandatory access controls and the user privilege model—it allows files within Time Machine backups to be deleted only by programs related to Time Machine.

From the command line, no user—not even one logged in as root—can delete files in a Time Machine backup. Time Machine uses this strict policy because it uses new file system features in Leopard Server. The policy prevents corruption in the backup directory by preventing tools from deleting files from backups, because some tools may not recognize the new file system features.

Mandatory access controls are integrated with the exec system service to prevent the execution of unauthorized applications. This is the basis for application controls in parental controls in Leopard and managed preferences in Leopard Server.

Mandatory access controls enable strong parental controls. In the case of the new sandboxing facility, mandatory access controls restrict access to system resources as determined by a special sandboxing profile that is provided for each sandboxed application. This means that even processes running as root can have extremely limited access to system resources.

Sandboxing

Sandboxing helps ensure that applications do only what they're intended to do by placing controls on applications that restrict what files they can access, whether the applications can communicate over the network, and whether the applications can be used to launch other applications.

In Leopard Server, many of the system's helper applications that normally communicate with the network—such as mDNSResponder (the software underlying Bonjour) and the Kerberos KDC—are sandboxed to guard them from abuse by attackers trying to access the system.

In addition, other programs that routinely take untrusted input (for instance, arbitrary files or network connections) such as Xgrid and the Quick Look and Spotlight background daemons are sandboxed.

Sandboxing is based on the system's mandatory access controls mechanism, which is implemented at the kernel level. Sandboxing profiles are developed for each application that runs in a sandbox, describing precisely which resources are accessible to the application.

Managed Preferences

Managed Preferences provide computer administrators with tools to enforce policy. Administrator users can use features like Simple Finder to limit the launching of a set of applications or they can create a whitelist of web sites that users can visit. This is the kind of simple interface that administrators of a public library or computer environment can use to restrict access to applications or sites to keep users from performing malicious activities.

In Leopard Server, you use Workgroup Manager to manage preferences for users of Leopard systems.

Quarantine Applications

Applications that download files from the Internet or receive files from external sources (such as mail attachments) can use the Quarantine feature to provide a first line of defense against malicious software such as Trojan horses. When an application receives an unknown file, it adds metadata (quarantine attributes) to the file using new functions found in Launch Services.

Files downloaded using Safari, Mail, and iChat are tagged with metadata indicating that they are downloaded files and refer to the URL, date, and time of the download. This metadata is propagated from archives that are downloaded (such as ZIP or DMG files) so that any file extracted from the archive is also tagged with the same information. This metadata is used by the download inspector to prevent dangerous file types from being opened unexpectedly.

The first time you try to run an application that has been downloaded, download inspector inspects the file, asks whether you want to run the application, and displays the information on the date, time, and location of the download.

You can continue to open the application or cancel the attempt, which is appropriate if you don't recognize or trust the application. After an application is opened, this message does not appear again for that application and the quarantine attributes are lifted.

This new mechanism dramatically reduces the number of warnings related to downloads that you see. Such messages now appear only when you attempt to launch a downloaded application. When you do see a warning, you are given useful information about the source of the download that can help you make an informed decision about whether to proceed.

Application-Based Firewall

A new application-based firewall makes it easier for nonexperts to get the benefits of firewall protection. The new firewall allows or blocks incoming connections on a per-application basis, rather than on a per-port basis.

Users can restrict firewall access to essential network services (such as those needed for DHCP, BOOTP, IPSec VPNs, and Bonjour), or they can allow (or block) access to selected applications on an individual basis. The application firewall uses digital signatures to verify the identity of applications. If you select an unsigned application, Leopard Server signs that application to uniquely identify it.

For expert users, the IPFW firewall is still available on the system. Because IPFW handles packets at the protocol-layer of the networking stack and the application firewall is a application layer filter, the IPFW rules take precedence.

Signed Applications

By signing applications, your Mac can verify the identity and integrity of an application. All applications shipped with Leopard Server are signed by Apple. In addition, third-party software developers can sign their software for the Mac. Application signing doesn't provide intrinsic protection, but it integrates with several other features to enhance security.

Features—such as parental controls, managed preferences, Keychain, and the firewall—use application signing to verify that the applications they are working with are the correct, unmodified versions.

With Keychain, the use of signing dramatically reduces the number of Keychain dialogs presented to users because the system can validate the integrity of an application that uses the Keychain. With parental controls and managed preferences, the system uses signatures to verify that an application runs unmodified.

The application firewall uses signatures to identify and verify the integrity of applications that are granted network access. In the case of parental controls and the firewall, unsigned applications are signed by the system on an ad hoc basis to identify them and verify that they remain unmodified.

Smart Card Unlock of FileVault and Encrypted Storage

Smart cards enable you to carry your digital certificates with you. With Leopard, you can use your smart card whenever an authentication dialog is presented.

Leopard Server has the following four token modules to support this robust, two-factor authentication mechanism and Java Card 2.1 standards:

- Belgium National Identification Card (BELPIC)
- Department of Defense Common Access Card (CAC)
- Japanese government PKI (JPKI)
- U.S. Federal Government "Personal Identity Verification also called FIPS-201 (PIV)

Other commercial Smart Card vendors provide token modules to support integrations of their Smart Card with the Mac OS X Smart Card architecture.

Similar to an ATM card and a PIN code, two-factor authentication relies on something you have and something you know. If your smart card is lost or stolen, it cannot be used unless your PIN is also known.

Leopard has additional functionality for smart card use, such as:

- Lock system on smart card removal. You can configure your Mac to lock the system when you remove your smart card.
- Unlock keychain. When you insert a smart card, the keychain can be unlocked, and your stored information and credentials can be used.
- Unlock FileVault. You can use smart card to unlock your FileVault encrypted home directory. You can enable this function by using a private key on a smart card.

Sharing and Collaboration Services

In Leopard Server, you can enable and configure sharing services to allow access only to users that you specify through access control lists (ACLs). You can create user accounts for sharing based on existing user accounts on the system, and for entries in your address book. Sharing services become more secure with ACLs.

Enhanced Encrypted Disk Image Cryptography

The Disk Utility tool included in Leopard enables you to create encrypted disk images—using 128-bit (default) or even stronger 256-bit AES encryption—so you can safely mail valuable documents, files, and folders to friends and colleagues, save the encrypted disk image to CD or DVD, or store it on the local system or a network file server. FileVault also uses this same encrypted disk image technology to protect user folders.

A disk image is a file that appears as a volume on your hard drive. It can be copied, moved, or opened. When the disk image is encrypted, files or folders placed in it are encrypted.

To see the contents of the disk image, including metadata such as file name, date, size, or other properties, a user must enter the password or have a keychain with the correct password.

The file is decrypted in real time, only as the application needs it. For example, if you open a QuickTime movie from an encrypted disk image, Leopard decrypts only the portion of the movie currently playing.

Enhanced VPN Compatibility and Integration

Leopard Server includes a universal VPN client with support built into the Network preferences pane, so you have everything you need to establish a secure connection. The VPN client supports L2TP over IPSec and PPTP, which makes Apple's VPN client compatible with the most popular VPN servers, including those from Microsoft and Cisco.

You can also use digital certificates and one-time password tokens from RSA or CryptoCARD for authentication in conjunction with the VPN client. The one-time password tokens provide a randomly generated passcode number that must be entered with the VPN password—a great option for those who require extremely robust security.

In addition, the L2TP VPN client can be authenticated using credentials from a Kerberos server. In either case, you can save the settings for each VPN server you routinely use as a location, so you can reconnect without needing to reconfigure your system each time.

Apple's L2TP VPN client can connect you to protected networks automatically by using its VPN on demand feature. VPN on demand can detect when you want to access a network that is protected by a VPN server and can start the connection process for you. This means that your security is increased because VPN connections can be closed when not in use, and you can work more efficiently.

In Leopard Server, the VPN client includes support for Cisco Group Filtering and DHCP over PPP to dynamically acquire additional configuration options such as static routes and search domains.

Improved Secure Connectivity

VPN support has been enhanced to connect to more of the most popular VPN servers—without additional software.

Installing Leopard Server

2

Use this chapter to customize the default installation of Leopard Server for your specific network security needs.

By securely configuring the different stages of the installation process and understanding Leopard Server permissions, you can make sure that your computer is hardened to match your security policy.

Important: When possible, computers should remain isolated from the operational network until they are completely and securely configured. Use an isolated test network for installation and configuration.

System Installation Overview

Although a secure configuration of an existing Leopard Server installation is possible, securely configuring a fresh installation is simpler. This might not always be practical, but it is the recommended way to configure Leopard Server.

The preinstallation of Leopard Server on a new computer is not locked down from a security standpoint. This is by design, because a server is used to administer an entire network and typically needs additional services. If a previous installation of Leopard Server exists on a computer, consider a clean installation of Leopard Server by doing an Erase and Install or by reformatting the volume.

WARNING: The Erase and Install option completely erases the content of a volume. Be sure to back up your files before continuing.

When backing up and restoring information, use the following guidelines:

- Back up only user files and data. Restoring system settings might change the system configuration.
- Reinstall applications from the original media. Do not restore them from a backup.

When you configure your new partitions, you should securely erase the partition that you're installing Leopard Server on. For more information, see "Securely Erasing Data" on page 169.

If you decide against securely erasing the partition, securely erase free space after installing Leopard Server. For more information, see "Using Disk Utility to Securely Erase a Disk or Partition" on page 170.

There are several ways to install the operating system, depending on your environment and installation strategy. These include:

- Installing locally from DVD
- Installing locally from another partition or disk
- Installing remotely from an administrator computer

Disabling the Firmware Password

Before installing Leopard, disable the Open Firmware password (for PowerPC-based computers) or the Extensible Firmware Interface (EFI) password (for Intel-based computers).

Disabling the Firmware Password (PPC-Based Computers)

If Leopard is already installed, use the Firmware Password Utility to disable the firmware password.

To disable the Open Firmware password:

1. Restart the computer while holding down the Command, Option, O, and F keys.
2. When prompted, enter the Open Firmware password.

 If you are not prompted to enter a password, the Open Firmware password is disabled.
3. Enter the following commands:

```
reset-nvram
reset-all
```

Disabling the Firmware Password (Intel-Based Computers)

If you are using an Intel-based Macintosh computer use the Firmware Password Utility to disable the EFI password.

For more information about the Firmware Password Utility, see "Using the Firmware Password Utility" on page 87.

Preparing an Administrator Computer

You can use an administrator computer to install, set up, and administer Leopard Server on another computer. An administrator computer is a computer with Leopard or Leopard Server that you use to manage remote servers.

When you install and set up Leopard Server on a computer that has a display and keyboard, it's already an administrator computer. To make a computer with Leopard into an administrator computer, you must install additional software.

Important: If you have administrative applications and tools from Mac OS X Server version 10.4 Tiger or earlier, do not use them with Leopard.

To enable remote administration of Leopard Server from a Leopard computer:

1. Make sure the computer has Leopard installed.
2. Make sure the computer has at least 1 GB of RAM and 1 GB of unused disk space.
3. Insert the Administration Tools CD.
4. Open the Installers folder.
5. Open ServerAdministrationSoftware.mpkg to start the Installer, and then follow the onscreen instructions.

The Server Installation Disc

You can install the server software using the Mac OS X Server Install Disc. This installation disc contains everything you need to install Leopard Server. It also contains an Other Installs folder, which has installers for upgrading a Leopard computer to Leopard Server and for separately installing server administration software, the Directory application, the Podcast Capture application, X11 software, and Xcode developer tools.

In addition to the installation disc, Leopard Server includes the Administration Tools CD. You use this disc to set up an administrator computer. This disc also contains installers for the Directory application, the Podcast Capture application, and the QuickTime Streaming Server (QTSS) Publisher application. For advanced administrators, this disc contains installers for PackageMaker and Property List Editor.

Setting Up Network Services

Before you can install, you must set up or have the following settings for your network service:

- **Domain Name System (DNS):** You must have a fully qualified domain name for each server's IP address in DNS. The DNS zone must have the reverse-lookup record for the name and address pair. Not having a stable, functioning DNS system with reverse lookup leads to service failures and unexpected behaviors.

 The standalone server setup choice in the assistant will set up a local DNS server and configure the server to look at 127.0.0.1 for DNS. This zone will not recurse to any other server setup and will assume that it is authoritative for the zone entered during setup.

- **Dynamic Host Configuration Protocol (DHCP):** Avoid assigning dynamic IP addresses to servers. If your server gets its IP address through DHCP, set up a static mapping in the DHCP server, so your server gets the same IP address every time (via its Ethernet address).

- **Firewall or routing:** In addition to any firewall running on your server, the subnet router might have network traffic restrictions in place. Make sure your server's IP address is available for the traffic you are planning to handle and the services you are planning to run.

Connecting to the Directory During Installation

If you want to use a server as an Open Directory master, make sure it has an active Ethernet connection to a secure network before installation and initial setup.

Installing Server Software on a Networked Computer

When you start up a computer from a server installation disc, SSH starts so that remote installations can be performed.

Important: Before you install or reinstall Leopard Server, make sure the network is secure. Secure Shell (SSH) gives others access to the computer over the network. For example, design the network topology so you can make the server computer's subnet accessible only to trusted users.

Starting Up for Installation

The computer can't install to its own startup volume, so you must start up in some other way, such as:

- Optical Media, DVDs
- Alternate volumes (second partitions on the hard disk or external FireWire disks)
- Netboot

The computer must install from the same disk or image that started up the computer. Mounting another share point with an installer won't work. The installer uses some of the files currently active in the booted system partition for the new installation.

Before Starting Up

If you're performing a clean installation rather than upgrading an existing server, back up user data on the disk or partition where you're installing the server software to an encrypted storage device or to storage media stored in a secured area.

If you're upgrading an existing server, make sure that saved setup data won't be inadvertently detected and used to automatically set up an advanced configuration. Server Assistant looks for saved setup data on all mounted disks and in all directories the server is configured to access. The saved setup data overwrites the server's existing settings.

Remotely Accessing the Install DVD

When used as the startup disc, the Install DVD provides some services for remote access. After you start up from the DVD, SSH and Virtual Network Computing (VNC) are available for use.

VNC enables you to use a VNC viewer (like Apple Remote Desktop) to view the user interface as if you were using the remote computer's keyboard, mouse, and monitor. All the things you could do at the computer using the keyboard and mouse are available remotely, as well as locally. This excludes hard resets, other hardware manipulation, or holding down keys during startup.

SSH enables you to have command-line access to the computer, with administrator privileges.

Important: To securely and remotely install Leopard Server, perform the installation in a trusted environment.

To access the computer with VNC:

1. Start the target server from the Install DVD for Leopard Server or later.

 The procedure you use depends on the target server hardware.

 To learn more about startup disk options, see "Starting Up for Installation" on page 39.

2. Establish an SSH tunnel between the local host and the remote server to securely perform the installation by redirecting the VNC traffic through the tunnel.

 For example, to redirect Apple Remote Desktop traffic through an SSH tunnel, enter:

   ```
   ssh -v -L 2501:local_host:5900 target_server -l target_server_username
   ```

3. Use your VNC viewer software to open a connection to the target server.

4. Identify the target server.

 If the VNC viewer includes the target server in a list of available servers, select it in the list. Otherwise, enter an IP address in IPv4 format (000.000.000.000).

 If you don't know the IP address and the remote server is on the local subnet, use the `sa_srchr` command to identify computers on the local subnet where you can install server software. Enter the following from an existing computer with Mac OS X Server Tools installed:

   ```
   /System/Library/Serversetup/sa_srchr 224.0.0.1
   ```

 This command returns the IP address and the EthernetID (in addition to other information) of servers on the local subnet that started up from the installation disk.

5 When prompted for a password, enter the first eight digits of the server's built-in hardware serial number.

To find a server's serial number, look for a label on the server.

If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

If you're using Apple Remote Desktop as a VNC viewer, enter the password but don't specify a user name.

Important: This password is valid only during setup.

To access the computer with SSH:

1 Start the target computer from the Install DVD for Leopard Server or later.

The procedure you use depends on the target server hardware.

To learn more about startup disk options, see "Starting Up for Installation" on page 39.

2 Use the Terminal to open an SSH connection to the target server.

The user name is root and the password is the first eight digits of the server's built-in hardware serial number.

To find a server's serial number, look for a label on the server. If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

Important: This password is valid only during setup.

If you don't know the IP address and the remote server is on the local subnet, you can use the `sa_srchr` command to identify computers on the local subnet where you can install server software. Enter the following from an existing computer with Mac OS X Server Tools installed:

```
/System/Library/Serversetup/sa_srchr 224.0.0.1
```

This command returns the IP address and EthernetID (in addition to other information) of servers on the local subnet that started up from the installation disk.

Starting Up from the Install DVD

The easiest and most secure way to install Leopard Server is to install it physically at the computer, known as a local installation, using the DVD. When performing a local installation, it is recommended, if applicable, that the entire drive be reformatted using at least a 7-pass secure erase, rather than only reformatting the partition where Leopard Server is to be installed, in case sensitive information was left on the other partitions.

If the target server is an Xserve with a built-in DVD drive, start the server using the Install DVD by following the instructions in the *Xserve User's Guide* for starting from a system disc.

If the target server has no built-in DVD drive, you can use an external FireWire DVD drive. You can also install server software on an Xserve system that lacks a DVD drive by moving its drive module to another Xserve system that has a DVD drive.

If your server has multiple partitions and you are only installing on a partition, you should still perform a secure erase of that partition. This type of installation is known as a clean installation. After the drive is securely erased and formatted, partitions can be created as required.

When installing the Leopard Server, only install the packages that are needed. All data on the target drive is lost during the installation.

> ***WARNING:*** The following instructions cause all information about the target volume (disk or partition) to be lost. Back up any data on the volume that should be retained.

To start up the computer with the installation disc:

1. Turn on the computer and insert the Leopard Server installation disc into the DVD drive.
2. If you're using a built-in DVD drive, restart the computer while holding down the C key.

 You can release the C key when you see the Apple logo.

 Alternatively, restart the computer by holding down the Option key, selecting the icon representing the installation disc, and then clicking the right arrow.

 You must use this method if you are starting up from an external DVD drive.

 If you're installing on an Xserve, see the *User's Guide* or *Quick Start* that came with your Xserve and follow the instructions to start up the installation.
3. After the computer restarts, choose the language you want to use during installation and then click the arrow button.

 The Installer is now running.
4. When the Installer opens, choose Utilities > Open Disk Utility to securely erase the target disk before proceeding.

 To securely erase and format the disk or partition, use Disk Utility. For more information, see "Using Disk Utility to Securely Erase a Disk or Partition" on page 170.

Starting Up from an Alternate Partition

For a single-server installation, preparing to start up from an alternate partition can be more time-consuming than using the Install DVD. The time required to image, scan, and restore the image to a startup partition can exceed the time taken to install once from the DVD.

However, if you are reinstalling regularly, or if you are creating an external Firewire drive-based installation to take to various computers, or if you need some other kind of mass distribution (such as clustered Xserves without DVD drives installed), this method can be very efficient.

Note: When creating a bootable external disk, you can use the Apple Partition Map (APM) format with Leopard Server to create a universal boot disk that will function on PowerPC and Intel hardware. The Leopard Server installer DVD is an APM disk. However, strictly speaking, only the GUID Partitioning format is supported on Intel-based Macs and only APM is supported on Power-PC Macs.

This method is suited to installing on computers that you might not have easy physical access to. With sufficient preparation, this method can be modified for easy mass deployment of licensed copies of Leopard Server.

To use this method, you must have an existing installation on the computer. It is intended for environments where a level of existing infrastructure of Leopard Server is present, and might be unsuitable for a first-server installation.

To start from an alternate partition, there are four basic steps.

Step 1: Prepare the disks and partitions on the target computer

Before you proceed, you must have at least two partitions on the target computer. The first is going to be the initial and the final startup partition.

The second is the temporary installer partition. You can use a single disk with multiple partitions, or you can use multiple disks. You use Disk Utility to prepare the disks.

For more information about preparing and partitioning a hard disk, see the Disk Utility help.

Step 2: Create a restorable image of the Install DVD

This step doesn't need to be performed on the target computer. It can be done on an administrator computer, but there must be enough free space to image the entire Install DVD.

To create an image of the Install DVD:

1. Insert the Install DVD.
2. Launch Disk Utility.

3 Select the first session icon under the optical drive icon.

This is in the list of devices on the left side of the window.

4 Select File > New > Disk Image from <device>.

Note: Consider creating a disk image from a folder because it is more efficient. For more information, see the `asr` man page.

5 Give the image a name, select Read-only, Read/Write, or Compressed as the image type, and then click Save.

6 After the image is complete, select the image from list on the left.

7 In the menu, select Images > Scan Images for Restore.

8 Provide an administrator login and password as needed.

The installer disk image can now be restored to your extra partition.

From the Command Line

To use the command line, use `hdiutil` to create the disk image, and `asr` to scan the image for restore. All commands must be done with super-user or root privileges. For example, this command creates a disk image "Installer.dmg" from the device at disk1s1:

```
sudo hdiutil create -srcdevice disk1s1 Installer.dmg
```

This command scans the image "Installer.dmg" and readies it for restore:

```
sudo asr imagescan --source Installer.dmg
```

Step 3: Restore the image to the alternate partition

You can restore the disk image to a partition of the computer or to an external hard disk. When complete, the restored partition functions like the Install DVD. Make sure the alternate partition is at least the size of the disk image.

Restoring the disk image to the partition erases existing data on the partition.

To restore the image:

1 Start up the target computer.

2 Make sure the image does not reside on the partition that is to be erased.

3 Launch Disk Utility.

4 In the list of devices on the left side of the window, select the installer DVD image.

5 Click Restore.

6 From the left side of the window drag the installer image to the Source field.

7 From the list of devices on the left side of the window drag the alternate partition to the Destination field.

8 Select Erase Destination.

9 Unmount both volumes to perform a block-level restore.

If you don't unmount both volumes, `asr`, which does the copying, falls back to the slower file-copy mode.

10 Click Restore.

From the Command Line

If you prefer to use the command-line, you use the asr tool to restore the image to the partition. Using asr requires the use of superuser or root privileges. The basic syntax is:

```
sudo asr restore -s <compressedimage> -t <targetvol> --erase
```

For example, restoring an image called "Installer.dmg" to the partition "ExtraHD" would be:

```
asr restore -s Installer.dmg -t ExtraHD --erase
```

For more information about asr and its capabilities, see the tool's man page.

You can use `asr` to restore a disk over a trusted network, multicasting the blocks to client computers. Using the multicast server feature of asr, you could put a copy of the installer image on a partition of all computers that can receive the multicast packets. To successfully configure this, you'll need the information in the tool's man page.

The `asr` tool can also fetch the target image from an HTTP server using http or https URLs as its source, so the image doesn't need to reside on the target computer. However, there is a 2 GB file size limit. Also, if you use an older web server such as Apache 1.3, you must segment the image.

Step 4: Select the alternate partition as the startup disk

After the partition is restored, you can use it as a startup and installer disk for your server. Start up the computer from that partition. After the computer is up and running, it is a Leopard Server installer, exactly as if you had started the computer from the DVD.

To start up the computer with the installation disc:

1 Turn on the computer and hold down the Option key.

2 Select the icon representing the installation partition and then click the right arrow.

You must use this method if you are starting up from an external DVD drive.

If you're installing on an Xserve, the procedure for starting up from a DVD might be different. For more information, see the *Xserve User's Guide* or *Quick Start* that came with your Xserve.

3 After the computer restarts, choose the language you want to use during installation, and click the arrow button.

The Installer is now running.

From the Command Line

If you prefer to do this at the command-line, you can set the startup volume using the `systemsetup` tool. In versions of Tiger Server or later, the systemsetup tool is at /usr/sbin/systemsetup.

If you are using the Leopard client during this process, the tool is at /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Support/systemsetup.

You'll need to use the `-liststartupdisks`, and `-setstartupdisk` command options to find the newly restored installer volume, and select it as the startup disk. All commands issued with `systemsetup` must be run with superuser or root privileges.

The following is an example command to select the startup disk:

```
systemsetup -setstartupdisk "/Volumes/Mac OS X Server Install Disk"
```

Then issue the `sudo shutdown -r` *`time`* command to restart.

For more information about `systemsetup` and `shutdown`, see *Command-Line Administration* and the tool's man page.

Starting Up from a NetBoot Environment

If you have an existing NetBoot infrastructure, this is the easiest way to perform mass installation and deployment. This method can be used for clusters that have no optical drive or existing system software.

This method can also be used in environments where large numbers of servers must be deployed in an efficient manner.

This section won't tell you how to create the NetBoot infrastructure. If you want to set up NetBoot and NetInstall options for your network, servers, and client computers, see *System Imaging and Software Update Administration*.

This section has instructions to create a NetInstall image from the Mac OS X Server Install Disk, and start a server from it. There is no need to make preparations to the hard disk.

Step 1: Create a NetInstall image from the Install DVD

This step doesn't need to be done on the target computer. It can be done on an administrator computer that has enough free space to image the entire Install DVD.

1. Launch System Image Utility, in /Applications/Server/.
2. Select the Install DVD on the left, and choose NetInstall image on the right.
3. Click Continue.
4. Enter a name for the image, and a description.

 This information is seen by clients selecting it a startup disk.
5. Click Create and then choose a protected and safe location for the disk image.

Upon completion, this image can be used with an existing NetBoot server to start up a server for installation.

You can provide another level of protection of the disk image by generating a SHA-1 digest of the image and store the digest in a secure place. When needed, you can use the digest to verify the integrity of the image.

For more information about NetInstall images and System Image Utility, including customization options, see *System Imaging and Software Update Administration*.

Step 2: Start up the computer from the NetBoot server on a secure network

Use one of the following methods, depending on your environment.

- In the target computer GUI, select the NetInstall disk from the Startup Disk pane of the System Preferences.
- Restart the computer, holding down the "n" key.

 The first NetBoot server to respond to the computer starts up the computer with its default image.
- Restart the computer, holding down the Option key.

 The computer shows you available startup disks, locally on the computer and remotely from NetBoot and NetInstall servers. Select a disk and continue the startup.
- Use the command line locally or remotely to specify the NetBoot server that the computer will start up from:

 sudo bless --netboot --server bsdp://server.example.com

Preparing Disks for Installing Leopard Server

Before performing a clean installation of Leopard Server, you can partition the server computer's hard disk into multiple volumes, create a RAID set, or erase the target disk or partition.

If you're using an installation disc for Leopard Server or later, you can perform these tasks from another networked computer using VNC viewer software, such as Apple Remote Desktop, before beginning a clean installation.

> ***WARNING:*** Before partitioning a disk, creating a RAID set, or erasing a disk or partition on a server, preserve user data you want to save by copying it to another disk or partition.

Choosing a File System

A file system is a method for storing and organizing computer files and the data they contain on a storage device such as a hard disk. Leopard Server supports several kinds of file systems. Each file system has its own strengths. You must decide which system fits your organization's needs.

For more information, see developer.apple.com/technotes/tn/tn1150.html.

The following systems are available for use:

The Mac OS Extended (Journaled) aka HFS+J File System
An HFS+J volume is the default file system for Leopard Server.

An HFS+J volume has an optional journal to speed recovery when mounting a volume that was not unmounted safely (for example, as the result of a power outage or crash). The journal makes it quick and easy to restore the volume structures to a consistent state, without scanning structures.

The journal is used only for volume structures and metadata. It does not protect the contents of a fork. In other words, this journal protects the integrity of the underlying disk structures, but not data that is corrupted due to a write failure or catastrophic power loss.

More information about HFS+J can be found in Apple's Developer Documentation at:

developer.apple.com/documentation/MacOSX/Conceptual/BPFileSystem/Articles/Comparisons.html

The Mac OS Extended (Journaled, Case-Sensitive) aka HFSX File System
HFSX is an extension to HFS Plus and allows volumes to have case-sensitive file and directory names. Case-sensitive names means that you can have two objects whose names differ only by the case of the letters, in the same directory at the same time. For example, you could have Bob, BOB, and bob in the same directory as uniquely named files.

A case-sensitive volume is supported as a boot volume format. An HFSX file system for Leopard Server must be specifically selected when erasing a volume and preparing for initial installation. HFSX is an available format for the "erase and install" option for local installs. HFSX is *not* an available format for remotely controlled installations. If you are planning to use NFS, use case-sensitive HFSX.

An HFSX volume can be case-sensitive or case-insensitive. Case sensitivity (or lack thereof) is global to the volume. The setting applies to all file and directory names on the volume.

To determine whether an HFSX volume is case sensitive, check whether it appears as Mac OS Extended or Mac OS X Extended (case-sensitive) in Disk Utility. Alternatively, run the following command to see if it creates one or two files.

```
$ touch aaaa AAAA
```

If the volume is not case sensitive, only one file (aaaa) is created in the current directory.

Note: An HFSX volume might not be case-sensitive. Additionally, your third-party software solutions might not work correctly with case sensitivity.

Important: Case-sensitive names do not ignore Unicode ignorable characters. This means that a single directory can have several names that would be considered equivalent using Unicode comparison rules, but they are considered distinct on a case-sensitive HFSX volume.

Partitioning a Hard Disk

Partitioning the hard disk creates a volume for server system software and additional volumes for data and other software. Partitioning erases previous contents of the disk.

The minimum recommended size for an installation partition is 20 GB. A larger volume is recommended for a standard or workgroup configuration because they keep shared folders and group websites on the startup volume together with the server software.

Erasing a disk is another way of saying that you have given a disk a single volume partition and erased that volume.

Consider dedicating a hard disk or a volume of a partitioned hard disk to server software. Put additional software, share points, websites, and so forth on other disks or volumes. With this approach, you can upgrade or reinstall the server software without affecting your other software or user data and you can improve performance by relieving the Input/Output connection.

If you must store additional software or data on the system volume, consider mirroring it to another drive.

Note: Having an extra, empty partition or two on the target installation disk can give you additional flexibility in installation and deployment. For example, additional space can give you a place to temporarily mirror your current installation before performing an in-place update, or it can give you a fast installer disk.

Partitioning a Disk Using Disk Utility

You can use the Installer to open the Disk Utility application and then use Disk Utility to erase the installation target volume or another volume.

You can erase the target volume using the Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, and Mac OS Extended (Journaled, Case-Sensitive) format.

You cannot partition the active startup disk or erase the active startup volume.

1 Launch Disk Utility.

If you are in the Installer, Disk Utility is available from the Utilities menu.

Otherwise, launch the application from /Applications/Utilities/Disk Utility.

2 Select the disk to be partitioned.

You can't select your current startup disk. Selecting a volume on the disk allows you to erase the volume but does not create a different partition scheme.

3 Click Partition.

4 Choose your partition scheme and follow the instructions in the window to set all necessary parameters.

5 Click Apply.

You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Macintosh computer with Leopard and choose Help > Disk Utility Help.

Partitioning a Disk Using the Command Line

You can use the diskutil command-line tool to partition and erase a hard disk. Normally, you would use a remote shell (SSH) to log in to the newly started computer to use this method. The tool to partition disks is `diskutil`.

In the same manner as using Disk Utility, you can erase the target volume using the Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, and Mac OS Extended (Journaled, Case-Sensitive) format.

You cannot partition the active startup disk or erase the active startup volume.

All potentially destructive diskutil operations must be done with superuser or root privileges.

Additional information about diskutil and other uses can be found in *Command-Line Administration*. For complete command syntax for `diskutil`, consult the tool's man page.

The specific command issued depends on your disk format needs and the hardware in use. Take care to use command-line arguments that apply to your specific needs.

The following command is a sample, which partitions a computer's only 120 GB hard disk into two equal 60 GB journaled HFS+ volumes ("BootDisk" and "DataStore"), which can start up a PowerPC-based Macintosh computer.

The basic syntax is:

```
diskutil partitionDisk device numberOfPartitions APMFormat <part1Format
     part1Name part1Size> <part2Format part2Name part2Size>
```

So the command is:

```
diskutil partitionDisk disk0 2 APMFormat JournaledHFS+ BootDisk 50%
     JournaledHFS+ DataStore 50%
```

Creating a RAID Set

If you're installing Leopard Server on a computer with multiple internal hard disks, you can create a Redundant Array of Independent Disks (RAID) set to optimize storage capacity, improve performance, and increase reliability in case of a disk failure.

For example, a mirrored RAID set increases reliability by writing your data to two or more disks at once. If one disk fails, your server uses one of the other disks in the RAID set.

You can use Disk Utility to set up a RAID set. There are two types of RAID sets and one additional disk option available in Disk Utility:

- **A striped RAID set (RAID 0)** splits files across the disks in the set. A striped RAID set improves the performance of your software because it can read and write on all disks in the set at the same time. You might use a striped RAID set if you are working with large files, such as digital video. However, RAID 0 will not provide any additional protection for your data. The loss of one drive will result in the loss of all data.
- **A mirrored RAID set (RAID 1)** duplicates files across the disks in the set. Because this scheme maintains two or more copies of the files, it provides a continuous backup of them. In addition, it can help keep data available if a disk in the set fails. Mirroring is recommended if you have shared files or applications that must be accessed frequently.

 To prevent data loss, set up RAID mirroring before installing Leopard Server.
- **A concatenated disk** set lets you use several disks as a single volume. This is not a true RAID set and offers no redundancy or performance increase.

You can combine RAID sets to combine their benefits. For example, you can create a RAID set that combines the fast disk access of a striped RAID set and the data protection of a mirrored RAID set. To do this, create two RAID sets of one type and then create a RAID set of another type, using the first two RAID sets as the disks.

The RAID sets you combine must be created with Disk Utility or `diskutil` in Tiger or later.

You cannot mix the method of partitioning used on the disks in a RAID set. (The PPC platform is APMFormat and the Intel platform is GPTFormat.)

Mac Pro desktop computers and Intel-based Xserves can boot from a software RAID volume. Some Intel-based Macs do not support booting from software RAID volumes. If you try to start these Intel-based Macs from a software RAID volume, the computer might start up with a flashing question mark.

The following computers do not support booting from software RAID volumes:

- iMac (early 2006)
- Mac mini (early 2006)

No PowerPC-based Macs support booting from software RAID volumes.

If you need more sophisticated RAID support, consider a hardware RAID. It has specially dedicated RAID hardware and can contain over 5 terabytes of storage.

Creating a RAID Set Using Disk Utility

You can use the Installer to open Disk Utility and then use Disk Utility to create the RAID set from available disks. Creating a RAID set erases the contents of the disks involved, so it isn't necessary to erase the disks before creating the RAID set.

RAID set volumes can be Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, Mac OS Extended (Journaled, Case-Sensitive) format, and MS-DOS FAT format. For more information about volume formats, see "Preparing Disks for Installing Leopard Server" on page 47.

You cannot create a RAID set from the startup disk.

To create a RAID set using Disk Utility:

1. Launch Disk Utility.

 If you are in the Installer, Disk Utility is available from the Utilities menu; otherwise, launch the application from /Applications/Utilities/Disk Utility.

2. Select the disk to be part of the RAID set.

 You can't select your startup disk.

 When creating RAID sets or adding disks, specify the entire disk instead of a partition on that disk.

3. Click RAID.
4. Choose your RAID set type.
5. Drag the disks to the window.
6. Follow the instructions in the window to set parameters.
7. Click Create.

 You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Macintosh computer with Leopard and choose Help > Disk Utility Help.

From the Command Line

You can use the diskutil command-line tool to create a RAID set. Normally, you would use a remote shell (SSH) to log in to the newly-started computer to use this method.

You can use `diskutil` to can create a RAID volume that is Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, Mac OS Extended (Journaled, Case-Sensitive) format, or MS-DOS FAT format. However keep in mind the following:

- You cannot create a RAID from the startup disk.
- When creating RAID sets or adding disks, specify the entire disk instead of a partition on that disk.
- All potentially destructive diskutil operations must be done with superuser or root privileges.

Additional information about diskutil and other uses can be found in *Command-Line Administration*. For complete command syntax for diskutil, consult the tool's man page.

Use command-line arguments that apply to your specific needs. The following command is a sample, which creates a single mirrored RAID set (RAID 1) from the first two disks installed in the computer (disk0 and disk1), with the resulting RAID volume called MirrorData.

The basic syntax is:

```
diskutil createRAID mirror setName format device1 device2 …
```

So the command is:

```
diskutil createRAID mirror MirrorData JournaledHFS+ disk0 disk1
```

Erasing a Disk or Partition

You have several options for erasing as disk, depending on your preferred tools and your computing environment:

- **Erasing a disk using the Installer:** You can erase a disk or partition while using the Mac OS X Server Installer. When you select the target volume in the Installer, you can also select an option to have the target disk or partition erased during installation using the Mac OS Extended (Journaled) format. This is the recommended format for a Leopard Server startup volume.
- **Erasing a disk using Disk Utility:** You can use the Installer to open Disk Utility and then use it to erase the target volume or another volume. You can erase the target volume using the Mac OS Extended format or Mac OS Extended (Journaled) format. You can erase other volumes using either of those formats, Mac OS Extended format (Case-Sensitive) format, or Mac OS Extended (Journaled, Case-Sensitive) format.

 You can erase but not partition a disk or partition while using the Mac OS X Server Installer. When you select the target volume in the Installer, you can also select an option to have the target disk or partition erased during installation using the Mac OS Extended (Journaled) format. This is the recommended format for a Leopard Server startup volume.

You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Macintosh computer with Leopard and choose Help > Disk Utility Help.

- **Erasing a disk using the command line:** You can use the command line to erase disks using the tool diskutil. Erasing a disk using diskutil results in losing all volume partitions. The command to erase a complete disk is:

  ```
  diskutil eraseDisk format name [OS9Drivers | APMFormat | MBRFormat |
     GPTFormat] device
  ```

 For example:

  ```
  diskutil eraseDisk JournaledHFS+ MacProHD GPTFormat disk0
  ```

 There is also an option to securely delete data by overwriting the disk with random data multiple times. For more details, see diskutil's man page.

 To erase a single volume on a disk, a slightly different command is used:

  ```
  diskutil eraseVolume format name device
  ```

 For example:

  ```
  diskutil eraseVolume JournaledHFS+ UntitledPartition /Volumes/
     OriginalPartition
  ```

Additional information about diskutil and other uses can be found in *Command-Line Administration*. For complete command syntax for diskutil, consult the tool's man page.

Identifying Remote Servers When Installing Leopard Server

For remote server installations, you need to know this information about the target server:

- **The identity of the target server:** When using Server Assistant, you must be able to recognize the target server in a list of servers on your local subnet or you must enter the IP address of the server (in IPv4 format: 000.000.000.000) if it resides on a different subnet. Information provided for servers in the list includes IP address, host name, and Media Access Control (MAC) address (also called hardware or Ethernet address).

 If you use VNC viewer software to remotely control installation of Leopard Server or later, it might let you select the target server from a list of available VNC servers. If not, enter the IP address of the server (in IPv4 format: 000.000.000.000).

 The target server's IP address is assigned by a DHCP server on the network. If no DHCP server exists, the target server uses a 169.xxx.xxx.xxx address unique among servers on the local subnet. Later, when you set up the server, you can change the IP address.

If you don't know the IP address and the remote server is on the local subnet, you can use the `sa_srchr` command to identify computers on the local subnet where you can install server software. Enter the following from an existing computer with Mac OS X Server Tools installed:

```
/System/Library/Serversetup/sa_srchr 224.0.0.1
```

This command returns the IP address and the EthernetID (in addition to other information) of servers on the local subnet that have started up from the installation disk.

Important: Sever Assistant uses Bonjour to look for services on the same subnet and generates IPv4 and IPv6 traffic in the process. To prevent IPv6 traffic, disable IPv6.

- **The preset password for the target server:** The password consists of the first eight digits of the server's built-in hardware serial number. To find a server's serial number, look for a label on the server. Older computers have no built-in hardware serial numbers. For these systems, use 12345678.

 Important: This password is valid only during setup.

Installing Server Software Interactively

You can use the installation disc to install server software interactively on a local server, on a remote server, or on a computer with Leopard pre-installed.

Installing Locally from the Installation Disc

You can install Leopard Server directly onto a computer with a display, a keyboard, and an optical drive attached.

If you have an Install DVD, the optical drive must be able to read DVD discs.

You can also install directly onto a computer that lacks a display, keyboard, and optical drive capable of reading your installation disc. In this case, you start the target computer in target disk mode and connect it to an administrator computer using a FireWire cable.

You use the administrator computer to install the server software on the target computer's disk or partition, which appears as a disk icon on the administrator computer.

These instructions assume you have started up the computer using the Install DVD, installer partition, or NetInstall disk. If you have not, see the relevant instructions beginning at "Starting Up for Installation" on page 39.

To install server software locally:

1. After the computer starts, choose the language you want the server to use and click Continue.

2 When the Installer opens, use the Utilities menu to open Disk Utility to securely erase the target disk before proceeding.

To securely erase and format the entire disk or partition, use Disk Utility. For more information, see "Using Disk Utility to Securely Erase a Disk or Partition" on page 170.

3 Proceed through the Installer's panes by following the onscreen instructions.

4 When the Select a Destination pane appears, select a target disk or volume (partition) and make sure it's in the expected state.

If you're doing a clean installation, click Options to format the destination disk or volume in Mac OS Extended (Journaled) format. Select Erase to format the disk in Mac OS Extended (Journaled) format; then click OK.

If the volume you select contains Mac OS X Server v10.3.9 or v10.2.8 and you want to upgrade, click Options, select "Don't erase" and then click OK.

Important: When you perform an upgrade, make sure that saved setup data won't be inadvertently detected and used by the server. If saved setup data is used, the server settings are not compatible with the saved settings and can cause unintended consequences. For more information, see *Server Administration*.

5 At the "Install" screen, click Customize.

6 Deselect options not needed on this server.

It is recommended to not install unneeded languages.

Note: By default, X11 is not selected. The X11 X Window system provides the ability to run X11-based applications under Leopard Server. Although this capability can be useful, it introduces configuration and security issues.

7 Click the Printer Drivers disclosure triangle to reveal printer drivers, and deselect drivers you don't need.

Printer drivers can always be installed later if a printer is added.

Install only drivers for the printers that will be used.

8 Proceed through the Installer's panes by following the onscreen instructions.

After installation is complete, the computer restarts and you can perform initial server setup.

9 If you're using an administrator computer to install onto a server that's in target disk mode and connected using a FireWire cable:

a Quit Server Assistant when it starts automatically on the administrator computer.

b Shut down the administrator computer and the server.

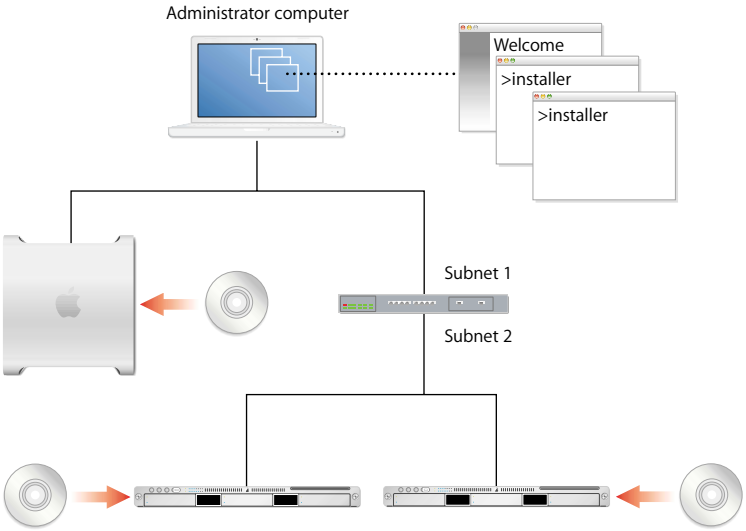
c Start up the administrator computer and the server normally (not in target disk mode).

Now you can use Server Assistant from the administrator computer to remotely set up the server.

To set up a server locally or remotely, see *Server Administration*.

Installing Remotely with Server Assistant

To install Leopard Server on a remote server from the server Install DVD, installation partition, or NetInstall disk, you need an administrator computer from which to use Server Assistant to manage the installation, as shown here.



After the computer starts up, you can control and manage other servers from an administration computer in a secure environment.

Important: If you have administrative applications and tools from Server Tiger or earlier, do not use them with Leopard Server.

To use the Installer user interface, use VNC to view and interact with the remote installer. For more information, see "Installing Remotely with VNC" on page 58.

These instructions assume you have started up the computer using the Install DVD, installer partition, or NetInstall disk. If you have not, see the instructions at "Starting Up for Installation" on page 39.

You don't need to be an administrator on the local computer to use Server Assistant.

To install on a remote server by using Server Assistant:

1. After the target computer has started from the server Install DVD, installation partition, or NetInstall disk, launch Server Assistant in the /Applications/Server/ folder on the administrator computer.
2. Select "Install software on a remote server."

3 For every target server, identify the server and add it to the list.

If it's on the local subnet, select it in the list; otherwise, click the Add (+) button and enter an IP address in IPv4 format (000.000.000.000).

If you already have a saved server list, load it now by selecting File > Load Server List.

4 When prompted for a password, enter the first eight digits of the server's built-in hardware serial number.

To find a server's serial number, look for a label on the server.

If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

5 After you finish adding servers to the list, save this list for future use by selecting File > Save Server List.

6 Proceed by following the onscreen instructions.

7 When the Volumes pane appears, select a target disk or volume (partition), make sure it's in the expected state, and click Continue.

If the volume you select contains Mac OS X Server v10.4.11 or v10.3.9 and you want to upgrade, select "Don't erase." Otherwise, select Erase to format the disk in Mac OS Extended (Journaled) format; then click OK.

WARNING: When you perform an upgrade, make sure that saved setup data won't be detected and used by the server. If saved setup data is used, the server settings are not compatible with the saved settings and can cause unintended consequences. For more information, see *Server Administration*.

8 Proceed by following the onscreen instructions.

While installation proceeds, you can open another Server Assistant window to install server software on other computers. Choose File > New Window to do so.

After installation is complete, the target server restarts and you can perform initial server setup. *Server Administration* describes how.

Installing Remotely with VNC

If you're using an installation disc for Leopard Server or later, you can control installation from another computer using open source VNC viewer software or Apple Remote Desktop. This allows you to remotely control preparation of the target disk or partition before beginning installation.

You can partition the hard disk into multiple volumes, create a RAID set, or erase the target disk or partition.

The process for remotely installing with VNC is the same as installing locally at the keyboard and monitor, except that you must first connect to the VNC server on the target computer with a VNC client, like Apple Remote Desktop.

For information about connecting to a computer running from an Install DVD, see "Remotely Accessing the Install DVD" on page 40.

For information about running the installer locally, see "Installing Locally from the Installation Disc" on page 55.

Installing Server Software from an Image

You can install and reinstall the server software with a known good and secure configuration that you previously set up on a model server using disk images.

Before creating the disk image, you might also want to securely configure additional server settings as described in the other chapters of this guide. Make sure the model server you are imaging meets the security requirements of your organization and is thoroughly tested.

For information about how to create and install server software with disk images, see *Getting Started*.

Secure erase can be done before or after installation. It's best to do it before installation to ensure that old data is overwritten and not recoverable. Before installing server software from a disk image, securely erase the physical disk or partition that the image is being installed on using at least a 7-pass erase. For more information, see "Securely Erasing Data" on page 169.

Using the installer Command-Line Tool to Install Server Software

You use the `installer` tool to install server software on a local or remote computer from the command-line. For information about installer:

- See *Command-Line Administration*.
- Open the Terminal application and enter `installer`, `installer -help`, or `man installer`.

These instructions assume you have started up the computer using the Install DVD, installer partition, or NetInstall disk. If you have not, see the relevant instructions beginning at "Starting Up for Installation" on page 39.

If you follow the instructions for performing a clean installation, back up the user files you want to preserve, then use `diskutil` to securely erase (7-pass or 35-pass) the volume and format it to enable journaling.

To securely erase a volume with 7-pass erase:

```
$ diskutil secureErase 2 "/Volumes/Mount 01"
```

For more information, see "Securely Erasing Data" on page 169. You can also use `diskutil` to partition the volume and to set up mirroring. For more information, see the `diskutil` man page.

Important: It is not recommended to you store data on the hard disk or hard disk partition where the operating system is installed. This prevents you from losing data if you need to reinstall or upgrade system software. If you must store additional software or data on the system software partition, consider mirroring the drive.

To use installer to install server software:

1. Start a command-line session with the target server by choosing from the following:
 - Installing a local server: When the Installer opens, choose Utilities > Open Terminal to open the Terminal application.
 - Installing a remote server: From Terminal on an administrator computer or from a UNIX workstation, establish an SSH session as the root user with the target server, substituting the target server's actual IP address for <ip address>:

     ```
     ssh root@<ip address>
     ```

 If you don't know the IP address and the remote server is on the local subnet, use the `sa_srchr` command to identify computers on the local subnet where you can install server software:

   ```
   /System/Library/Serversetup/sa_srchr 224.0.0.1
   mycomputer.example.com#PowerMac4,4#<ip address>#<mac address>#Mac OS X
        Server 10.5#RDY4PkgInstall#2.0#512
   ```

 You can also use Server Assistant to generate information for computers on the local subnet. Open Server Assistant, select "Install software on a remote computer," and click Continue to access the Destination pane and generate a list of servers awaiting installation.
2. When prompted for a password, enter the first eight digits of the server's built-in hardware serial number.

 To find a server's serial number, look for a label on the server. If the target computer is set up as a server, you'll also find the hardware serial number in /System/Library/Serversetup/SerialNumber.

 If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

3 Identify the target-server volume where you want to install the server software.

To list the volumes available for server software installation from the installation disc, enter this command:

```
/usr/sbin/installer -volinfo -pkg /System/Installation/Packages/
     OSInstall.mpkg
```

You can also identify a NetInstall image you've created and mounted:

```
/usr/sbin/installer -volinfo -pkg /Volumes/ServerNetworkImage10.5/
     System/Installation/Packages/OSInstall.mpkg
```

The list displayed reflects your environment, but here's an example showing three available volumes:

```
/Volumes/Mount 01
/Volumes/Mount1
/Volumes/Mount02
```

4 If you haven't already done so, prepare the disks for installation.

For more information about preparing disks for installation, see "Preparing Disks for Installing Leopard Server" on page 47.

If the target volume has Mac OS X Server v10.4.10 or 10.3.9 installed, when you run `installer` it upgrades the computer to Leopard Server and preserves user files.

If you're performing a clean installation, back up the user files you want to preserve, then use `diskutil` to erase the volume and format it to enable journaling:

```
/usr/sbin/diskutil eraseVolume HFS+ "Mount 01" "/Volumes/Mount 01"
/usr/sbin/diskutil enableJournal "/Volumes/Mount 01"
```

You can also use `diskutil` to partition the volume and set up mirroring. For more information about the command, see the `diskutil` man page.

Important: It is recommended not to store data on the hard disk or hard disk partition where the operating system is installed. This prevents you from losing data if you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.

5 Install the operating system on a volume from the list generated in step 3.

For example, to use Mount 01 in the example in step 3 to install from a server installation disc, enter:

```
/usr/sbin/installer -verboseR -lang en -pkg /System/Installation/
     Packages/OSInstall.mpkg -target "/Volumes/Mount 01"
```

If you're using a NetInstall image, the command identifies them as step 3 shows.

When you enter the -lang parameter, use one of the following values: en (for English), de (for German), fr (for French), or ja (for Japanese).

During installation, progress information appears. While the installation proceeds, you can open another Terminal window to install server software on another computer.

6 When installation from the disc is complete, restart the server by entering:

```
/sbin/reboot
```

or

```
/sbin/shutdown -r time
```

Server Assistant opens when installation is complete. You can now proceed to set up the server. For more information, see *Server Administration*.

Installing Multiple Servers

To initiate multiple server software installations, you can use Server Assistant, VNC viewer software, or the `installer` tool. After using Server Assistant to initiate server software installation on more than one remote computer, you can choose File > New Window to install the software on another batch of computers.

When running Server Assistant from an administration computer to install on multiple machines, group the same hardware configurations together. For example, choose all Intel-based Xserve machines or all G4 Mac minis.

After using a VNC viewer to control installation of Leopard Server or later on a remote computer, you can use the VNC viewer to open a connection to another remote computer and control installation on it. Because this involves interacting with each server individually, it is a less efficient method of installing on multiple servers.

The most efficient method of installation would be completely automated. Opening the Terminal application and using the `installer` tool to initiate each server software installation doesn't accomplish this efficiently. However, scripting the command-line tool (using known values for server IP addresses, for example) to automate multiple simultaneous installations can be very efficient. To completely automate server installation, you must script the `installer` tool and have a high measure of control over the network infrastructure.

For example, to have known IP addresses and the relevant hardware serial numbers included in your script, you cannot rely on the randomly assigned IP addresses. You can use DHCP assigned static addresses to remove that uncertainty and ease your scripting considerations.

The methods, scripting languages, and possibilities are too many to list in this guide.

Upgrading a Computer from Leopard to Leopard Server

You can use the Install DVD for Leopard Server to upgrade a desktop computer that has the following characteristics:

- Has Leopard or later installed
- Has an Intel processor
- Was introduced in summer 2006 or later
- Meets the system requirements

To upgrade a computer from Leopard to Leopard Server:

1. Start up the computer from the hard disk, as you would for normal use.

 Do not use an installation disc.

2. Insert the Install DVD, open the Other Installs folder, and double-click MacOSXServerInstall.mpkg to run the Installer.

 When the Installer finishes, your computer restarts and Server Assistant opens to let you set up the server.

3. After the server restarts, use Software Update to install server software updates.

How to Keep Current

After you've set up your server, you'll want to update it when Apple releases server software updates.

There are several ways to access update releases of Leopard Server:

- In Server Admin, select a server in the Servers list, then click the Server Updates button.
- Use the Software Update pane of System Preferences.
- Use the `softwareupdate` command-line tool.
- Use the server's software update service.
- Download a disk image of the software update from www.apple.com/support/downloads.

Using Interactive Server Setup

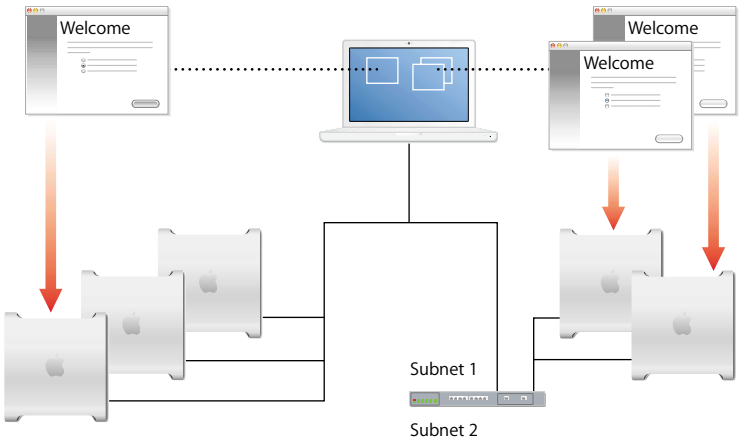
The simplest way to set up a small number of servers is to use Server Assistant's guided interview process after establishing a connection with each server in turn. You provide server setup data interactively, then initiate setup immediately. If you have only a few servers to set up, the interactive approach is useful.

You can use the interactive approach to set up a local server, a remote server, or several remote servers. To use this approach, open Server Assistant, connect to target servers, supply setup data, and then initiate the setup immediately.

This is the technique you use to set up a local server, as "Setting Up a Local Server Interactively" on page 66 describes. You can also use this interactive approach to set up a remote server from an administrator computer. For instructions, see "Setting Up a Remote Server Interactively" on page 67.

When multiple remote servers can use the same setup data, you can supply the data and then initiate setup of all servers at once, using a batch approach. When running Server Assistant from an administration computer to set up multiple servers, group the same hardware configurations together. For example, choose all Intel-based Xserve machines or all G4 Mac minis.

This technique, shown on the left side of the following illustration, requires that network identifiers for target servers be set using DHCP or BootP. For instructions, see "Setting Up Multiple Remote Servers Interactively in a Batch" on page 68.



To customize the setup of individual servers, you can manage each setup individually from a different Server Assistant window. This approach is shown on the right side of the illustration above. For instructions, see "Setting Up a Remote Server Interactively" on page 67.

Although the previous illustration shows target servers on the same subnet as the administrator computer in one scenario and target servers on a different subnet in the other scenario, both setup scenarios can be used to set up servers on the same and different subnets.

If a target server is on a different subnet, you must supply its IP address. Servers on the same subnet are listed by Server Assistant, so you select servers from a list.

To securely set up your server, note the following when providing information in the Assistant's panes:

- Password—The administrator password you specify during setup is also used for the root account. Because of this, take special care to ensure that this account is as secure as possible:
 - Limit the number of administrator accounts issues. This makes it easier to retain control over the computer and identify whether an activity noted in the logs was legitimate.
 - When entering administrator account information for the Name and the Short Name fields, use names other than "administrator," "admin," or some form of the word administrator. The name alone should not identify the account as an administrator account.
 - Use a strong password in the Password and Verify fields. Passwords can be up to 255 characters and contain uppercase letters, lowercase letters, numbers, and special characters. Choose a password that consists of at least 12 characters that would not be found in a dictionary, and that contains mixed-case letters, numbers, and special characters.
 - After setting up the administrator user, click Continue.
 - Change the root password as soon as possible after installation is complete.
- Computer Name and Local Hostname—The names should not indicate the purpose of the computer. The word "server" should not be used as the name or part of the name.
- Network interfaces—Select only those interfaces that will be used and deselect all others. For example, if the network interface for the server will be Built-in Ethernet only, deselect Built-in FireWire. Do not use AppleTalk. Do not enable Remote Management in the Network Names screen unless it is required.
- TCP/IP—For the Configure IPv4 setting, select "Manually." The use of DHCP or BootP is not recommended. Make sure that DHCP or DNS servers you specify for the server you're setting up to use are running.
- Directory usage—Set the "Set directory usage" setting to Standalone Server to simplify the installation. The type of directory usage depends on the role of the server being installed. For information about configuring directory usage, see Chapter 24, "Securing Directory Services."
- Server Configuration Mode—Choose Advanced for the Server Configuration Mode. This mode will result in a server installation with all services installed, but deactivated. The other two choices (Standard and Workgroup) will activate the services whose icons are shown. Services should only be activated when they are necessary.
- Services—Do not enable services. The services you enable depend on the role of the server being installed. Configure each service carefully before activation.

- Network time—Some authentication services, including Kerberos, require that time be synchronized across all computers, which necessitates synchronization with a timeserver. For security, one timeserver on the local network can synchronize with a trusted Internet timeserver, but it is the only server that should do so. Direct use of an Internet timeserver is not recommended for other servers.

 Note: If NTP is to be used on a network without Internet access, the server providing the NTP service must have another time source connected, such as a GPS unit, or must be set up to use an undisciplined local clock. See www.ntp.org.

- Setup data file—If you save the setup data in a file, encrypt it using the "Save in Encrypted Format" option.

Setting Up a Local Server Interactively

After you install server software, you can use the interactive approach to set it up locally if you have physical access to the computer.

Important: This setup assumes you are using the Advanced server configuration mode. It is recommended not to try to use these instructions with Standard or Workgroup modes.

To set up a local server interactively:

1. Fill out the Mac OS X Server Advanced Worksheet in *Server Administration*.

 When the server restarts, Server Assistant opens.

2. Enter the setup data you've recorded on the *Installation & Setup Worksheet* as you move through the Assistant's panes, following the onscreen instructions.

 Make sure that DHCP or DNS servers you specify for the server you're setting up to use are running.

 After you enter setup data, Server Assistant displays a summary of the data.

3. Review the setup data you entered and, if necessary, click Go Back to change it.

4. To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file or saved directory record), click Save As.

 To encrypt a configuration file or directory record, select "Save in Encrypted Format" and then enter and verify a passphrase. You must supply the passphrase before a target server can use an encrypted setup file.

5. To initiate setup of the local server, click Apply.

6. When server setup is complete, click Restart Now.

 Now you can log in as the server administrator user created during setup to configure services.

Setting Up a Remote Server Interactively

After server software is installed on a server, you can use the interactive approach to set it up remotely from an administrator computer that can connect to the target server.

To set up a remote server interactively:

1. Fill out the Mac OS X Server Advanced Worksheet in *Server Administration*.
2. Make sure the target server is running.
3. On an administrator computer, open Server Assistant in /Applications/Server/.

 You don't need to be an administrator on the administrator computer to use Server Assistant.
4. In the Welcome pane, select "Set up a remote server" and click Continue.
5. In the Destination pane, put a check in the Apply column for the remote server you want to set up, enter its preset password in the Password field, and click Continue to connect to the server.

 If you don't see the target server on the list, click Add to add it or Refresh to determine whether it's available.
6. For the server configuration type, select "Advanced."
7. In the Language pane, specify the language you want to use to administer the target server.
8. If you are using saved setup data, do the following:
 a. In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to use. If the saved setup data is encrypted, enter the passphrase when prompted.
 b. Optionally, choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.
9. If you are entering setup data, do the following:
 a. Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions, and click Continue.
 b. Make sure that the DHCP or DNS servers you specify for the server you're setting up are running.
10. After you specify setup data, review the summary displayed by Server Assistant and optionally click Go Back to change data.
11. To save the setup data as a text file or in a form you can use for automatic server setup (as a saved setup file or saved directory record), click Save As.

 To encrypt a configuration file or directory record, select "Save in Encrypted Format" and then enter and verify a passphrase.

 You must supply the passphrase before a target server can use an encrypted setup file.

12 To initiate setup of the remote target server, click Apply.

13 When server setup is complete, click Continue Now.

The target server restarts and you can log in as the server administrator user you created during setup to configure services.

Setting Up Multiple Remote Servers Interactively in a Batch

You can use the interactive approach to set up multiple servers as a batch if:

- The servers are accessible from an administrator computer
- The servers use the same chip platform (for example, Intel or PowerPC)
- The servers use the same setup data, except for server software serial numbers and network identities (host name, computer name, and local hostname)
- Network identities are provided by a DHCP or BootP server

When running Server Assistant from an administration computer to set up multiple servers, group the same hardware configurations together. For example, choose Intel-based Xserve machines or G4 Mac minis.

If you have servers with different configuration files, you can open a Server Assistant window for each server type. This way you can group servers by platform, settings, subnet, or other criteria you choose.

To set up multiple remote servers interactively in a batch:

1 Fill out the Mac OS X Server Advanced Worksheet in *Server Administration* with the settings you want to use for all servers you want to set up.

2 Make sure the target servers and DHCP or DNS servers you want them to use are running.

3 On an administrator computer that can connect to all target servers, open Server Assistant located in /Applications/Server/.

You don't need to be an administrator on the administrator computer to use Server Assistant.

4 In the Welcome pane, select "Set up a remote server" and click Continue.

5 In the Destination pane, put a check in the Apply column for each remote server you want to set up, enter the preset password in the Password field for each server, and click Continue to connect to the servers.

If your target server doesn't appear on the list, click Add to add it.

6 In the Language pane, specify the language you want to use to administer the target servers.

7 If you are using saved setup data, do the following:

a In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to use. If the saved setup data is encrypted, enter the passphrase when prompted.

b Optionally, choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.

8 If you are entering setup data, do the following:

a Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions, and click Continue.

b Make sure that DHCP or DNS servers you specify for the server you're setting up to use are running.

9 After setup data is specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.

10 To save the setup data as a text file or in a form you can use for automatic server setup (as a saved setup file or saved directory record), click Save As.

To encrypt a configuration file or directory record, select "Save in Encrypted Format" and then enter and verify a passphrase.

You must supply the passphrase before an encrypted setup file can be used by a target server.

11 To initiate server setup, click Apply.

12 To initiate setup of the remote target server, click Apply.

13 When server setup is complete, click Continue Now.

The target servers restart and you can log in as the server administrator user created during setup to configure their services.

Updating System Software

After installing Leopard Server, be sure to install the latest approved security updates. Leopard Server includes Apple Software Update, an application that downloads and installs software updates from Apple's Software Update server or from an internal software update server.

You can configure Software Update so that it checks for updates periodically or whenever you choose. You can also configure Software Update to download, but not install, updates, if you want to install them later.

Before installing updates, check with your organization for their policy on downloading updates. They might prefer that you use an internal software update server, which reduces the amount of external network traffic and allows the organization to prequalify software updates with organization configurations before updating individual computers.

Important: Security updates published by Apple contain fixes for security issues, and are usually released in response to a specific known security problem. Applying these updates is essential.

If Apple Software Update does not install an update that you request, contact your network administrator. Failure to update signifies that the requested update could be a malicious file.

Important: Before connecting to the Internet, ensure that your network services are securely configured. If you have not secured and validated your settings for network services, do not enable your network connection to install software updates. Until you have securely configured your network services settings, you are limited to using the manual method of installing software updates. For more information, see "Securing Software Update Preferences" on page 141.

Updating from an Internal Software Update Server

The computer automatically looks for software updates from an internal software update server. By using an internal software update server, you reduce the amount of data transferred outside of the network and your organization can control which updates can be installed on your computer.

If you run Software Update over a wireless or untrusted network, you run a chance of downloading malicious updates from a rogue software update server. However, Software Update will not install a package that has not been digitally signed by Apple before distribution.

If you connect your computer to a network that manages its client computers, the network can require that the computer use a specified software update server.

To specify your software update server:

```
$ defaults write com.apple.SoftwareUpdate CatalogURL
     http://swupdate.example.com:8088/index.sucatalog
```

Replace *swupdate.example.com* with the fully qualified domain name (FQDN) or IP address of your software update server.

Note: You can specify the software update server to use using Workgroup Manager, which allows you to manage Software Update preferences for multiple computers.

To delete the information about the software update server:

```
$ defaults delete com.apple.SoftwareUpdate CatalogURL
```

Updating from Internet-Based Software Update Servers

Software Update can periodically check the Internet for software updates. Instead of using your computer to check for and install updates, consider using a test computer to download updates and verify file integrity before installing updates. You can then transfer the update packages to your operational computer. See "Updating Manually from Installer Packages" on page 71.

To download and install software updates using Software Update:

1. Choose Apple (🍎) > Software Update.

 After Apple Software Update looks for updates to your installed software, it displays a list of updates. To get older versions of updates, go to the software update website at www.apple.com/support/downloads/.

2. Select the updates you want to install, and choose Update > Install and Keep Package.

 When you keep the package, it is stored in the /Library/Packages/ folder.

 If you do not want to install any of the updates, click Quit.

3. Accept the licensing agreements to start installation.

 Some updates might require your computer to restart. If, after installing updates, software update asks you to restart the computer, do so.

Important: Make sure updates are installed when the computer can be restarted without affecting the users accessing the server.

Updating Manually from Installer Packages

Software updates can be manually downloaded for Apple products from www.apple.com/support/downloads/ using a computer designated for downloading and verifying updates. The download should be done separately so that file integrity can be verified before the updates are installed.

You can review the contents of each security update before installing it. To see the contents of a security update, go to Apple's Security Support Page at www.apple.com/support/security and click the "Security Updates page" link.

To manually download, verify, and install software updates:

1. Go to www.apple.com/support/downloads/ and download the software updates on a computer designated for verifying software updates.

 Note: Updates provided through Apple Software Update might sometimes appear earlier than standalone updates.

2. Review the SHA-1 digest (also known as a checksum) for each update file downloaded, which should be posted online with the update package.

3. Check downloaded updates for viruses.

4 Verify the integrity of each update.

For more information, see "Verifying the Integrity of Software" on page 72.

5 Transfer the downloaded update packages from your test computer to your current computer.

The default download location for update packages is /Library/Packages/. You can transfer update packages to any location on your computer.

6 Double-click the package.

If the package is located within a disk image (dmg) file, double-click the dmg file, and then double-click the package.

7 Proceed through the installation steps.

8 Restart the computer, if requested.

Install the relevant software update and then install subsequent security updates. Leopard Server ensures that the updates are installed in order by release date, oldest to newest.

Verifying the Integrity of Software

Software images and updates can include an SHA-1 digest, which is also known as a checksum. You can use this SHA-1 digest to verify the integrity of the software. Software updates retrieved and installed automatically from Apple Software Update verify the checksum before installation.

To verify software integrity:

1 Open Terminal.

2 Use the `sha1` command to display a file's SHA-1 digest.

```
$ /usr/bin/openssl sha1 full_path_filename
```

Replace *`full_path_filename`* with the full path filename of the update package or image for which the SHA-1 digest is being checked.

If provided, the SHA-1 digest for each software update or image should match the digest created for that file. If it does not, the file was corrupted and a new copy should be obtained.

Repairing Disk Permissions

Permissions on files can sometimes be set incorrectly, especially during a software installation. Incorrect permissions can cause the computer to malfunction and even introduce security vulnerabilities. Repairing these permissions is recommended after performing any software installation on Leopard Server.

Important: Perform the procedure to repair disk permissions after every software installation, including the operating system, updates, and applications.

Kinds of Permissions

Before you change or repair disk permissions, you should understand the two kinds of file and folder permissions that Leopard Server supports:

- Portable Operating System Interface (POSIX) permissions—standard for UNIX operating systems
- Access Control Lists (ACLs) permissions—used by Leopard Server, which are compatible with Microsoft Windows Server 2003 and Microsoft Windows XP

Note: In this guide, the term "privileges" refers to the combination of ownership and permissions, while the term "permissions" refers only to the permission settings that each user category can have (Read & Write, Read Only, Write Only, and None).

POSIX Permissions Overview

POSIX permissions let you control access to files and folders. Every file or folder has read, write, and execute permissions defined for three categories of users (owner, group, and everyone). There are four types of standard POSIX access permissions that you can assign: Read & Write, Read Only, Write Only, and None.

For more information, see "Setting POSIX Permissions" on page 151.

ACL Permissions Overview

An ACL provides an extended set of permissions for a file or folder and enables you to set multiple users and groups as owners. An ACL is a list of access control entries (ACEs), each specifying the permissions to be granted or denied to a group or user, and how these permissions are propagated throughout a folder hierarchy. In addition, ACLs are compatible with Windows Server (2000, 2003, and 2008) and Windows XP, giving you added flexibility in a multiplatform environment.

ACLs enable you to define more detailed permissions when assigning privileges than POSIX permissions. For example, rather than giving a user full writing permissions, you can restrict him or her to the creation of only folders and not files.

If a file or folder has no ACEs defined for it, Leopard Server applies standard POSIX permissions. If a file or folder has one or more ACEs defined for it, Leopard Server starts with the first ACE in the ACL and works its way down the list until the requested permission is satisfied or denied.

After evaluating the ACEs, Leopard Server evaluates the standard POSIX permissions defined for the file or folder. Then, based on the evaluation of ACL and standard POSIX permissions, Leopard Server determines what type of access a user has to a shared file or folder.

For more information, see "Setting ACL Permissions" on page 155.

Using Disk Utility to Repair Disk Permissions

Installing software sometime causes file permissions to become incorrectly set. Incorrect file permissions can create security vulnerabilities. Disk Utility only repairs POSIX permissions or minimal ACL permissions.

Most software you install in Leopard Server is installed from package (.pkg) files. Each time something is installed from a package file, a Bill of Materials (.bom) file is stored in the packages receipt file. Each Bill of Materials file contains a list of files installed by that package, along with the proper permissions for each file.

When you use Disk Utility to verify or repair disk permissions, it reads the Bill of Materials files from the initial Leopard Server installation and compares its list to the permissions on each file listed. If the permissions differ, Disk Utility can repair them.

You should repair disk permissions if you are experiencing symptoms that indicate permission-related problems after installing software, software updates, or applications.

Note: If you've modified permissions for files in accordance with organizational policies, be aware that repairing disk permissions can reset those modified permissions to those stated in the Bill of Materials files. After repairing permissions, reapply the file permission modifications to stay within your organizational policies.

To repair disk permissions:

1. Open Disk Utility.
2. Select the partition you want to repair.

 Select a partition, not a drive. Partitions are contained within drives and are indented one level in the list on the left.
3. Click Repair Disk Permissions.

 If you do not select a partition, this button is disabled.
4. Choose Disk Utility > Quit Disk Utility.
5. Choose Installer > Quit Installer, and click Restart.

Protecting System Hardware

3

Use this chapter to learn how to protect and secure your system hardware.

After installing and setting up Leopard Server, make sure you protect your system hardware.

Protecting Hardware

The first level of security is protection from unwanted physical access. If someone can physically access a computer, it becomes much easier to compromise the computer's security. When someone has physical access to the computer, they can install malicious software or event-tracking and data-capturing services.

Use as many layers of physical protection as possible. Restrict access to rooms that contain computers that store or access sensitive information. Provide room access only to those who must use those computers. If possible, lock the computer in a locked or secure container when it is not in use, and bolt or fasten it to a wall or piece of furniture.

The hard disk is the most critical hardware component in your computer. Take special care to prevent access to the hard disk. If someone removes your hard disk and installs it in another computer, they can bypass safeguards you set up. Lock or secure the computer's internal hardware.

If you can't guarantee the physical security of the hard disk, consider using FileVault for each home folder. FileVault encrypts home folder content and prevents the content from being compromised. For more information, see "Encrypting Home Folders" on page 162.

If you have a portable computer, keep it secure. Lock it up or hide it when it is not in use. When transporting the computer, never leave it in an insecure location. Consider buying a computer bag with a locking mechanism and lock the computer in the bag when you aren't using it.

Preventing Wireless Eavesdropping

Most network environments have wired and wireless access to the network. Wireless access helps businesses or organizations offer mobility to users throughout their network.

Although wireless technology gives your network more flexibility with your users, it can cause security vulnerabilities you may be unaware of. It is recommended that wherever possible, wireless access be disabled for security reasons. When using a wireless access point, make sure you properly configure the security settings to prevent unauthorized users from attempting to access your network.

Your wireless access point should require encryption of the connection, user authentication (through the use of certificates or smart cards), and time-outs for connections.

By requiring an encrypted wireless connection, you can maintain the integrity and confidentiality of data being transmitted to your wireless access point. The use of certificates or smart cards helps to ensure the users' identity, that your users are who they say they are.

Also, setting a time-out that disconnects wireless user connections lasting longer than 8 to 10 hours prevents your network from being attacked by a computer that is connected through your wireless access point and left unattended.

If you need to use Wi-Fi, see *Mac OS X Security Configuration* for information about how to leverage 802.1X for securing your Wi-Fi traffic.

Understanding Wireless Security Challenges

Most Mac computers have a built-in wireless network card. Users can configure their computer to be a wireless access point in order to share their Internet connection with other users. However, such a wireless access point isn't usually secure, thereby creating a point of access for an attacker.

Anyone within wireless range can gain access to your network by using an authorized user's insecurely configured wireless LAN. These possible points of access can be very large, depending on the number of users with wireless technology on their computers.

The challenge arises when trying to prevent users from creating access points to your network or trying to identify where the access points are and who is attempting to use them.

Many organizations restrict the use of wireless technology in their network environment. However, most Mac computers have wireless capability built in, and simply turning it off may not meet your organization's wireless technology restrictions. You might need to remove components from Mac OS X to disable them from being turned on in System Preferences.

OS Components

Special hardware, such as wireless networking cards and audio/video components, need driver software that runs at the kernel level. This driver software is implemented as kernel extensions ("kexts") in Mac OS X, also known as OS components. These kernel extensions can be removed from Mac OS X to prevent the use of a piece of hardware.

Disabling or removing OS components or kernel extensions will alter the behavior or performance of the system.

Important: Mac OS X sometimes has updates to specific OS components. When your computer installs these updates the component is overwritten or reinstalled if it was previously removed. This then reenables the hardware you wanted disabled. When you install updates make sure that the installation does not reenable an OS component you wanted disabled.

Removing Wi-Fi Hardware

Use the following instructions for removing AirPort support. This task requires administrator privileges.

You can also have an Apple Authorized Technician remove AirPort hardware from your Apple computer.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for AirPort hardware:

1. Open the /System/Library/Extensions folder.
2. Drag the following files to the Trash:

 AppleAirPort.kext

 AppleAirPort2.kext

 AppleAirPortFW.kext
3. Open Terminal and enter the following command:

   ```
   $ sudo touch /System/Library/Extensions
   ```

 The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Leopard.
4. Choose Finder > Secure Empty Trash to delete the files.
5. Restart the system.

From the Command Line:

```
# ------------------------------------------------------------------
# Protecting System Hardware
# ------------------------------------------------------------------
# Securing Wi-Fi Hardware
# ----------------------
# Remove AppleAirport kernel extensions
srm -r /System/Library/Extensions/AppleAirPort.kext
srm -r /System/Library/Extensions/AppleAirPort2.kext
srm -r /System/Library/Extensions/AppleAirPortFW.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

Removing Bluetooth Support Software

Use the following instructions to remove Bluetooth® support for peripherals such as keyboards, mice, or phones. This task requires administrator privileges.

Note: You can use a policy to disable Bluetooth support by managing Bluetooth preferences in Workgroup Manager.

You can also have an Apple Authorized Technician remove the built-in Bluetooth hardware support from your Apple computer.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for Bluetooth:

1. Open the /System/Library/Extensions folder.
2. Drag the following files to the Trash:

 IOBluetoothFamily.kext

 IOBluetoothHIDDriver.kext
3. Open Terminal and enter the following command:

 `$ sudo touch /System/Library/Extensions`

 The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Leopard.
4. Choose Finder > Secure Empty Trash to delete the files.
5. Restart the system.

From the Command Line:

```
# Removing BlueTooth Software
# --------------------------
# Remove Bluetooth kernel extensions
srm -r /System/Library/Extensions/IOBluetoothFamily.kext
srm -r /System/Library/Extensions/IOBluetoothHIDDriver.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

Removing IR Support Software

Use the following instructions to remove IR hardware support. This task requires you to have administrator privileges.

You can also have an Apple Authorized Technician remove IR hardware from your Apple computer.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for IR hardware support:

1. Open the /System/Library/Extensions folder.
2. Drag the following file to the Trash:

 AppleIRController.kext
3. Open Terminal and enter the following command:

   ```
   $ sudo touch /System/Library/Extensions
   ```

 The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library) are deleted and rebuilt automatically by Mac OS X.
4. Choose Finder > Secure Empty Trash to delete the file.
5. Restart the system.

From the Command LIne:

```
# Removing IR Support Software
# ----------------------------
# Remove IR kernel extensions.
srm -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

Preventing Unauthorized Recording

You computer might be in an environment where recording devices, such as cameras or microphones are not permitted. You can protect your organization's privacy by disabling these devices. This task requires administrator privileges.

Note: Some organizations insert a dummy plug in to the audio input and output ports to ensure that the audio hardware is disabled.

Removing Audio Recording Support

Use the following instructions to remove support for the microphone.

You can also have an Apple Authorized Technician remove the built-in microphone hardware from your Apple computer.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for audio hardware:

1. Open the /System/Library/Extensions folder.
2. To remove support for audio components such as the microphone, drag the following files to the Trash:

 AppleOnboardAudio.kext

 AppleUSBAudio.kext

 AudioDeviceTreeUpdater.kext

 IOAudioFamily.kext

 VirtualAudioDriver.kext
3. Open Terminal and enter the following command:

   ```
   $ sudo touch /System/Library/Extensions
   ```

 The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt automatically by Leopard.
4. Choose Finder > Secure Empty Trash to delete the files.
5. Restart the system.

From the Command Line:

```
# Removing Audio Recording Software
# --------------------------------
# Remove Audio Recording kernel extensions
srm -r /System/Library/Extensions/AppleOnboardAudio.kext
srm -r /System/Library/Extensions/AppleUSBAudio.kext
srm -r /System/Library/Extensions/AppleDeviceTreeUpdater.kext
srm -r /System/Library/Extensions/IOAudioFamily.kext
srm -r /System/Library/Extensions/VirtualAudioDriver.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

Removing Video Recording Support Software

Use the following instructions to remove support for an external or built-in iSight camera.

Note: The support for external iSight cameras should be removed on all machines; removing only support for internal iSight cameras will still leave support for external cameras available.

These instructions do not remove support for internal iSight cameras shipping on some Macintosh systems. There is currently no way to disable this camera software without disabling all USB drivers, which also disables other peripherals such as the keyboard and mouse. This task requires you to have administrator privileges.

You can also have an Apple Authorized Technician remove the built-in video camera hardware from your Apple computer.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for video hardware:

1. Open the /System/Library/Extensions folder.
2. To remove support for the external iSight camera, drag the following file to the Trash:

 Apple_iSight.kext
3. To remove support for the built-in iSight camera:
 a. Control-click IOUSBFamily.kext and choose Show Package Contents.
 b. Open the /Contents/PlugIns/ folder.
 c. Drag the following file to the Trash:
 - AppleUSBVideoSupport.kext

4 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Leopard.

5 Choose Finder > Secure Empty Trash to delete the files.

6 Restart the system.

From the Command Line:

```
# Removing Video Recording Software
# --------------------------------
# Remove Video Recording kernel extensions.

# Remove external iSight camera.
srm -rf /System/Library/Extensions/Apple_iSight.kext

# Remove internal iSight camera.
srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/
     AppleUSBVideoSupport.kext

# Remove Extensions cache files.
touch /System/Library/Extensions
```

Preventing Data Port Access

You computer's data ports can be easily compromised if your machine is unattended for a long period of time or is stolen. To keep your machine from being compromised, always keep it in a locked environment or hidden when you are not using it.

You can protect your system by preventing an unauthorized user from using your data ports. This keeps them from booting to a different volume using a USB Flash drive, USB, or FireWire external hard drive. This task requires administrator privileges.

Also by setting a firmware password using the Firmware Password Utility, you can prevent a physical Direct Memory Access (DMA) attack over Firewire. When the firmware password is set, any external device is denied direct access to computer memory content. For more information about the Firmware Password Utility, see "Using the Firmware Password Utility" on page 87.

Securing USB Hardware

Use the following instructions to remove USB mass storage device input/output support such as USB Flash drives and external USB hard drives.

Note: You can use a policy to control access to USB storage devices by managing USB preferences in Workgroup Manager.

The removal of this kernel extension only affects USB mass storage devices. It does not affect other USB devices such as a USB printer, mouse, or keyboard. This task requires administrator privileges.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for specific hardware:

1. Open the /System/Library/Extensions folder.
2. To remove support for USB mass storage devices, drag the following file to the Trash:

 IOUSBMassStorageClass.kext
3. Open Terminal and enter the following command:

   ```
   $ sudo touch /System/Library/Extensions
   ```

 The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt automatically by Leopard.
4. Choose Finder > Secure Empty Trash to delete the file.
5. Restart the system.

From the Command Line:

```
# Removing USB Support
# --------------------
# Remove USB kernel extensions
srm -r /System/Library/Extensions/IOUSBMassStorageClass.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

Removing FireWire Support Software

Use the following instructions to remove Firewire input/output support for components such as an external Firewire hard disk. This task requires administrator privileges.

Important: Repeat these instructions every time a system update is installed.

To remove kernel extensions for certain hardware:

1. Open the /System/Library/Extensions folder.
2. To remove support for Firewire mass storage devices, drag the following file to the Trash:

 IOFireWireSerialBusProtocolTransport.kext

3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Leopard.

4 Choose Finder > Secure Empty Trash to delete the file.

5 Restart the system.

From the Command Line:

```
# Securing FireWire Hardware
# ----------------------------
# Remove FireWire kernel extensions
srm -r /System/Library/Extensions/IOFireWireSerialBusProtocolTransport.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

System Hardware Modifications

Removing the kernel extensions does not permanently disable components; however, administrative access is needed to restore and reload them.

Although disabling hardware in this manner is not as secure as physically disabling hardware, it is more secure than only disabling hardware through System Preferences. This method of disabling hardware components might not be sufficient to meet a site security policy. Consult operational policy to determine if this method is adequate.

Authorized AppleCare Certified Technicians

If your environment does not permit the use of the following hardware components, you must physically disable them:

- AirPort
- Bluetooth
- Microphone
- Camera IR Port

Important: Attempting to remove components without the use of an Apple Certified technician will void your warranty.

A limited number of Apple Certified technicians can remove preapproved components. An Apple Certified Technician can remove the component without voiding the warranty on your computer. After an Apple Certified Technician removes the component the technician logs a special note with Apple Care indicating that the computer has had a component properly removed. Most components removed by Apple technicians can be reinstalled if needed.

To locate a Certified Apple Technician go to www.apple.com/buy.

For more information, see your local Apple representative.

Note: If you are in a government organization and need a letter of volatility for Apple products, send your request to AppleFederal@apple.com.

Securing Global System Settings

4

Use this chapter to learn how to secure global system settings, secure Open Firmware and Leopard Server startup, and to use log files to monitor system activity.

After installing and setting up Leopard Server, make sure you protect your hardware and secure global system settings.

Securing System Startup

When a computer starts up, it first starts Extensible Firmware Interface (EFI) or Open Firmware. EFI is the software link between the motherboard hardware and the software operating system. Open Firmware is similar to EFI, but it runs on PowerPC-based Macintosh computers. EFI and Open Firmware determine which partition or disk to load Leopard from. They also determine whether the user can enter single-user mode.

Single-user mode logs in the user as root. This is dangerous because root user access is the most powerful level of access, and actions performed as root are anonymous.

If you create an Open Firmware or EFI password, you prevent users from accessing single-user mode. The password also stops users from loading unapproved partitions or disks and from enabling target disk mode at startup.

After creating an Open Firmware or EFI password, you must enter this password when you start the computer from an alternate disk (for situations such as hard disk failure or file system repair).

To secure startup, perform one of the following tasks:

- Use the Firmware Password Utility to set the Open Firmware password.
- Set the Open Firmware password within Open Firmware.
- Verify and set the security mode from the command line.

WARNING: EFI and Open Firmware settings are critical. Take great care when modifying these settings and when creating a secure Firmware password.

An Open Firmware password provides some protection but it can be reset if a user has physical access to the machine and can change the physical memory configuration of the machine.

Open Firmware password protection can be bypassed if the user changes the physical memory configuration of the machine and then resets the PRAM three times (by holding down Command, Option, P, and R keys during system startup).

For more information about Open Firmware password protection, see:

- AppleCare Knowledge Base article # 06482, "Setting up Open Firmware Password protection in Mac OS X 10.1 or later" (www.apple.com/support/)
- AppleCare Knowledge Base article # 07666, "Open Firmware: Password Not Recognized when it Contains the Letter 'U'" (www.apple.com/support/)

PowerPC-Based Systems

PowerPC-based computers use Open Firmware to control hardware. This is similar to the BIOS on an x86 PC. Open Firmware is the hardware base layer for Leopard and is a possible point of intrusion. By protecting it from unauthorized access, you can prevent attackers from gaining access to your computer.

Using the Firmware Password Utility

The Leopard installation disc includes Firmware Password Utility, which you can use to enable an Open Firmware or EFI password.

To use the Firmware Password Utility:

1. Log in with an administrator account and open the Firmware Password Utility (located on the Leopard installation disc in /Applications/Utilities/).
2. Click Change.
3. Select "Require password to change Open Firmware settings."

 To disable the Open Firmware or EFI password, deselect "Require password to change Open Firmware settings." You won't need to enter a password and verify it. Disabling the Open Firmware password is only recommended for installing Leopard.
4. In the Password and Verify fields, enter a new Open Firmware or EFI password, and click OK.

 This password can be up to eight characters.

 Do not use the capital letter "U" in an Open Firmware password. If you do, your password is not recognized during the startup process.
5. Close the Firmware Password Utility.

You can test your settings by attempting to start up in single-user mode. Restart the computer while holding down the Command and S keys. If the login window loads, changes made by the Firmware Password Utility were completed successfully.

Configuring Open Firmware Settings

You can securely configure Open Firmware settings by setting a firmware password.

These instructions only apply to PowerPC-based Macintosh computers. If you are using an Intel-based Macintosh computer, use the Firmware Password Utility instead.

> *WARNING:* Modifying critical system files can cause unexpected issues. Your modified files can also be overwritten during software updates. Make these modifications on a test computer first, and thoroughly test your changes every time you change your system configuration.

To configure Open Firmware settings in Open Firmware:

1. Restart the computer while holding down the Command, Option, O, and F keys.

 This loads Open Firmware.

2. At the following prompt, change the password:

   ```
   > password
   ```

3. Enter a new password and verify it when prompted.

 This password can be up to eight characters.

 Do not use the capital letter "U" in an Open Firmware password.

4. Enable command mode:

   ```
   > setenv security-mode command
   ```

 In command mode the computer starts up from the partition selected in the Startup Disk pane of System Preferences.

 You can also enable full mode. Full mode is more restrictive than command mode. After enabling full mode, Open Firmware commands require you to enter your Open Firmware password. This includes the `boot` command, so Leopard will not start up unless you enter `boot` and authenticate with the Open Firmware password.

 To enable full mode, enter:

   ```
   > setenv security-mode full
   ```

5. Restart the computer and enable Open Firmware settings with the following command:

   ```
   > reset-all
   ```

 The login window should appear after restarting.

To test your settings, attempt to start up in single-user mode. Restart the computer while holding down the Command and S keys. If the login window appears, your Open Firmware settings are set correctly.

Using Command-Line Tools for Secure Startup

You can also configure Open Firmware or EFI from the command line by using the `nvram` tool. However, only the `security-mode` environment variable can be securely set.

You can set the security mode to one of the following values:

- **None:** This is the default value of security mode and provides no security to your computers Open Firmware.
- **Command:** This value requires a password if changes are made to Open Firmware or a user attempts to start up from an alternate volume or device.
- **Full:** This value requires a password to start up or restart your computer. It also requires a password to make changes to Open Firmware.

For example, to set the `security-mode` to `full` you would use the following command:

```
$ sudo nvram setsecurity-mode = “Full”
```

Do not set the `security-password` variable with `nvram` because the password is visible when viewing the environment variable list. The `nvram` tool requires system administrator or root access to set environment variables.

To securely set the password for EFI, use the Firmware Password Utility.

From the Command Line:

```
# Securing Global System Settings
# ------------------------------------------------------------------------
# Configuring Open Firmware Settings
# ---------------------------------
# Secure startup by setting security-mode. Replace $mode-value with
# “command” or “full”.
nvram security-mode=”$mode-value”

# Verify security-mode setting.
nvram -p
```

Intel-Based Systems

Intel-based computers use EFI to control low-level hardware. EFI is similar to BIOS on an x86 PC and is the hardware base layer for Leopard computers with Intel processors. By protecting it from unauthorized access you can prevent attackers from gaining access to your computer.

EFI and PowerPC-based computers can use the Firmware Password Utility to password protect the hardware layer. For information on using the Firmware Password Utility, see "Using the Firmware Password Utility" on page 87.

Configuring Access Warnings

You can use a login window or Terminal access warning to provide notice of a computer's ownership, to warn against unauthorized access, or to remind authorized users of their consent to monitoring.

Important: Every service enabled on the system must have a banner that displays the relevant access warning before authentication. For more information about enabling banners for services, see the relevant man pages and open source projects.

Enabling Access Warnings for the Login Window

Before enabling an access warning, review your organization's policy for what to use as an access warning.

When a user tries to access the computer's login window (locally or through Apple Remote Desktop), the user sees the access warning you create, such as the following:

To create a login window access warning:

1. Open Terminal and verify that your logged-in account can use `sudo` to perform a `defaults write`.
2. Change your login window access warning:

   ```
   $ sudo defaults write /Library/Preferences/com.apple.loginwindow
        LoginwindowText "Warning Text"
   ```

 Replace *`Warning Text`* with your access warning text.
3. Log out to test your changes.

 Your access warning text appears below the Mac OS X subtitle.

From the Command Line:

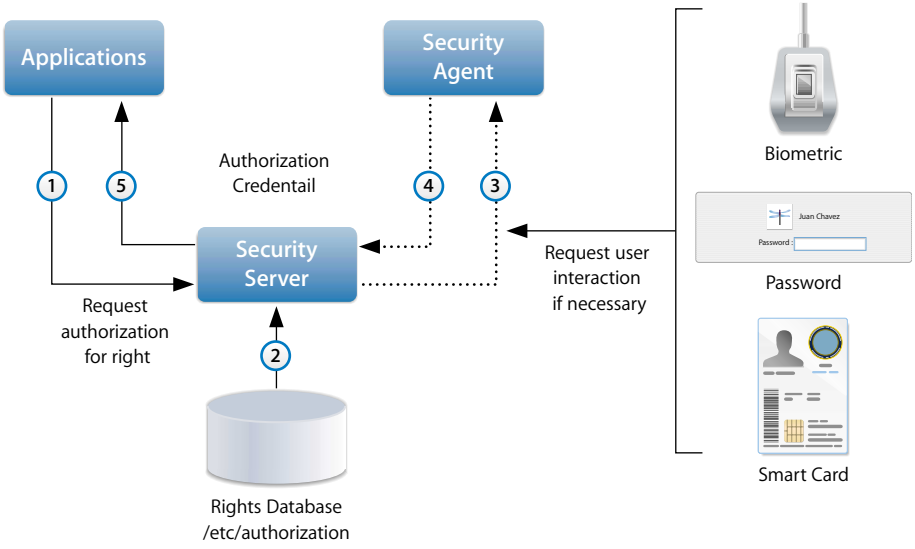
```
# Enabling Access Warning for the Login Window
# --------------------------------
# Create a login window access warning.
defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText
     "Warning Text"
# You can also used the BannerSample project to create an access warning.
```

AuthPlugin Architecture

AuthPlugins are used to control access to a service or application. The preinstalled AuthPlugins for Leopard are located in the /System/Library/CoreServices/SecurtiyAgentPlugins/ folder. These plug-ins, along with their associated rules and authorization rights for users, are defined in the /etc/authorization database, and are queried by the security server.

For more information about /etc/authorization, see “Managing Authorization Rights” on page 374.

The following graphic shows the workflow of the Security Server.



When an application requests authorization rights from the security server the security server interrogates the rights database (/etc/authorization) to determine the mechanisms to be used for authentication. If necessary, the security server requests user interaction through the security agent. The security agent then prompts the user to authenticate through the use of a password, biometric, or Smart Card device. Then the security agent sends the authentication information back to the security server, which passes it back to the application.

The BannerSample Project

If your computer has developer tools installed, the sample code for the banner sample project is located in /Developer/examples/security/bannersample. You can modify and customize this sample banner code for your organization.

After you compile the code you can place it in the /Library/Security/SecurityAgentPlugins/ folder. Then modify the key `system.login.console` in the /etc/authorization file using Terminal.

For more information about the bannersample, see the bannersample README file.

To modify the /etc/authorization file:

1. Open Terminal.
2. Enter the following command:

```
$ sudo pico /etc/authorization
```

3. Locate the `system.login.console` key.
4. Add `<string>bannersample:test</string>` above `<string> builtin:smartcard-siffer,privileged</string>`, as shown in bold below:

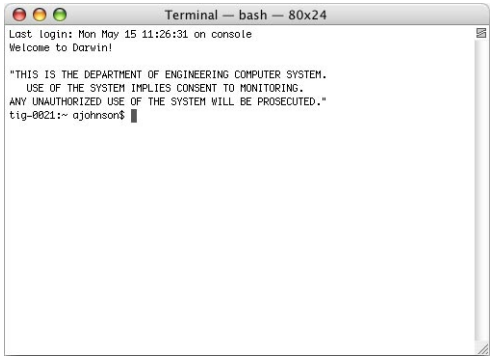
```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>comment</key>
<string>Login mechanism based rule. Not for general use, yet.</string>
<key>mechanisms</key>
<array>
<string>bannersample:test</string>
<string>builtin:smartcard-sniffer,privileged</string>
```

5. Save changes and exit the editor.
6. Restart the computer and verify that the banner appears.

Enabling Access Warnings for the Command Line

Before enabling an access warning, review your organization's policy for what to use as an access warning.

When a user opens Terminal locally or connects to the computer remotely, the user sees the access warning you create. The following task must be performed by an administrator user. You can use any text editor.



To create a command-line access warning:

1. Open Terminal.
2. Enter the following command to create the /etc/motd file:

   ```
   $ sudo touch /etc/motd
   ```

3. Enter the following command to edit the /etc/motd file:

   ```
   $ sudo pico /etc/motd
   ```

4. Enter in your access warning message.
5. Save changes and exit the text editor.
6. Open a new Terminal window to test changes.

 Your access warning text appears above the prompt in the new Terminal window.

Securing Local Server Accounts 5

Use this chapter to learn how to secure accounts by assigning user account types, by configuring directory access, by using strong authentication procedures, and by safely storing credentials.

Securing user accounts requires determining how accounts are used and setting the level of access for users.

When you define a user's account you specify the information to prove the user's identity, such as user name, authentication method (password, digital token, smart card, or biometric reader), and user identification number (user ID). Other information in a user's account is needed by various services—to determine what the user is authorized to do and to personalize the user's environment.

Types of User Accounts

When you log in to Mac OS X Server, you use a nonadministrator or administrator account. The main difference is that Mac OS X Server provides safety mechanisms to prevent nonadministrator users from editing key preferences and from performing actions critical to computer security. Administrator users are not as limited as nonadministrator users.

Nonadministrator and administrator accounts can be further defined by specifying additional user privileges or restrictions.

The following explains the types of user accounts.

User Account	User Access
Standard nonadministrator	Nonprivileged user access
Managed nonadministrator	Restricted user access
Server administrator	Administer the server configuration
Directory domain administrator	Administer the configured domains on the server
System administrator (root)	Unrestricted access to the server

Unless you need administrator access for specific system maintenance tasks that cannot be accomplished by authenticating with the administrator's account while logged in as a normal user, always log in as a nonadministrator user. Log out of the administrator account when you are not using the computer as an administrator. Never browse the web or check email while logged in to an administrator's account.

If you are logged in as an administrator, you are granted privileges and abilities that you might not need. For example, you can potentially modify system preferences without being required to authenticate. This authentication bypasses a security safeguard that prevents malicious or accidental modification of system preferences.

Note: This chapter describes how to secure local accounts configured on Leopard Server. For more information about securing user and group network accounts using Workgroup Manager, see Chapter 11, "Securing Accounts and Share Points."

Guidelines for Securing Accounts

When you create user accounts, follow these guidelines:

- Never create accounts that are shared by several users. Each user should have his or her own standard or managed account.

 Individual accounts are necessary to maintain accountability. System logs can track activities for each user account, but if several users share the same account it is difficult to track which user performed an activity. Similarly, if several administrators share an administrator account, it becomes harder to track which administrator performed an action.

 If someone compromises a shared account, it is less likely to be noticed. Users might mistake malicious actions performed by an intruder for legitimate actions by a user sharing the account.

- Each user needing administrator access should have an administrator account in addition to a standard or managed account.

 Administrator users should only use their administrator accounts for administrator purposes. By requiring an administrator to have a personal account for typical use and an administrator account for administrator purposes, you reduce the risk of an administrator performing actions like accidentally reconfiguring secure system preferences.

Defining User IDs

A user ID is a number that uniquely identifies a user. Mac OS X Server computers use the user ID to track a user's folder and file ownership. When a user creates a folder or file, the user ID is stored as the creator ID. A user with that user ID has read and write permissions to the folder or file by default.

The user ID is a unique string of digits between 500 and 2,147,483,648. New users created using the Accounts pane of System Preferences are assigned user IDs starting at 501.

It is risky to assign the same user ID to different users, because two users with the same user ID have identical directory and POSIX file permissions. However, each user has a unique GUID that is generated when the user account is created. Your GUID is associated with ACL permissions that are set on files or folders. By setting ACLs permissions you can prevent users with identical user IDs from accessing files and folders.

The user ID 0 is reserved for the root user. User IDs below 100 are reserved for system use; user accounts with these user IDs should not be deleted and should not be modified except to change the password of the root user.

If you don't want the user name to appear in the login window of a client computer, assign a user ID of less than 500 and enter the following command in a Terminal window:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow Hide500Users
     -bool YES
```

User names never appear in the login window in Leopard Server.

In general, after a user ID is assigned and the user starts creating files and folders, you shouldn't change the user ID.

One possible scenario in which you might need to change a user ID is when merging users created on different servers onto a new server or cluster of servers. The same user ID might have been associated with a different user on the previous server.

Securing the Guest Account

The guest account is used to give a user temporary access to your computer. The guest account should be disabled by default because it does not require a password to log in on the computer. If this account is enabled and is not securely configured, malicious users can gain access to your computer without the use of a password.

If you enable the guest account, enable parental controls (using Workgroup Manager) to limit what the user can do and disable access to shared files and folders by deselecting the "Allow guest to connect to shared folders" checkbox. If you permit the guest account to access shared folders, an attacker can easily attempt to access shared folders without a password.

When you finish with this account, disable it by deselecting the "Allow guests to log into this computer." This prevents the guest account from logging into the computer.

Securing Nonadministrator Accounts

There are two types of nonadministrator accounts: standard and managed.

- Standard users don't have administrator privileges and don't have parental controls limiting their actions.
- Managed users don't have administrator privileges but they have active parental controls. Parental controls help deter unsophisticated users from performing malicious activities. They can also help prevent users from misusing their computer.

Note: If your computer is connected to a network, a managed user can also be a user whose preferences and account information are managed through the network.

When creating nonadministrator accounts, restrict the accounts so they can only use what is required. For example, if you plan to store sensitive data on your local computer, disable the ability to burn DVDs.

Securing Administrator Accounts

Each administrator should have two accounts: a standard account for daily use and an administrator account for administrator access. Remember that the non-administrative account should be used for most daily activity, especially when accessing the network or Internet. The administrator's account should only be used when absolutely necessary to accomplish administrative tasks.

To secure administrator accounts, restrict the distribution of administrator accounts and limit the use of such accounts.

A user account with administrator privileges can perform standard user and administrator tasks such as:

- Creating user accounts
- Adding users to the Admin group
- Changing the FileVault master password
- Enabling or disabling sharing
- Enabling, disabling, or changing firewall settings
- Changing other protected areas in System Preferences
- Installing system software
- Escalating privileges to root

Securing the Directory Domain Administrator Account

A directory domain can reside on a computer running Leopard Server (for example, the LDAP folder of an Open Directory master, or other read/write directory domain) or it can reside on a non-Apple server (for example, a non-Apple LDAP or Active Directory server). Only a directory domain administrator can change the directory domain, including the managed accounts in the directory domain.

When configuring a directory domain administrator account, follow the same security guidelines as you would with any other administrator account.

You can modify the /etc/authorization configuration file to change authorizations for administrators and standard users.

To modify authorization by changing the /etc/authorization file:

1. Edit the /etc/authorization file using the `pico` tool, which allows for safe editing of the file.

 The command must be run as root:

   ```
   $sudo pico /etc/authorization
   ```

2. When prompted, enter the administrator password.

 This displays a property list for authorization, listing all available keys.

3. Locate the key you want to modify.

 For example, to change who has access to unlock the screensaver, modify the `system.login.screensaver` key by changing the rule:

   ```
   <key>rule</key>
     <string>authenticate-session-owner-or-admin</string>
   ```

 to

   ```
   <key>rule</key>
     <string>authenticate-session-owner</string>
   ```

 Doing this restricts the administrator from unlocking the screensaver.

4. Save and quit `pico`.

Securing the System Administrator Account

The most powerful user account in Leopard is the system administrator or root account. By default, the root account on Leopard Server is enabled and uses the same password as the first created admin user. You should disable it using the following command:

```
$ dsenableroot -d
```

Important: The system administrator or root account should only be used when absolutely necessary.

The root account is primarily used for performing UNIX commands. Generally, actions that involve critical system files require you to perform those actions as root. However, thanks to the sudo command, it is not necessary to leave the root account enabled in order to obtain root privileges.

If you are logged in as a Leopard Server administrator, you can perform commands with root privileges using the sudo command. You can use sudo to perform these commands even if the root account has been disabled. Leopard Server logs actions performed using the sudo command. This helps you track misuse of the sudo command and root privileges on a computer. Keep in mind that these logs can be edited if they are stored locally, so only grant sudo privileges to trusted users.

You can use the su command to log in to the command line as another user if you have that user's password. This includes the root user, if the root account is enabled. Once logged in as root, you can use the su command to change users without a password.

If you do decide to leave the root account disabled, you should still restrict access to the root account. If multiple users can log in as root, you cannot track which user performed root actions.

Do not allow direct root login, because the logs cannot identify which administrator logged in. Instead, log in using accounts with administrator privilege, and then use the sudo command to perform actions as root.

For instructions about how to restrict root user access in Directory Utility, open Mac Help and search for "Directory Utility."

Restricting sudo Usage

By default, sudo is enabled for administrator users. From the command line, you can disable root login or restrict the use of sudo. Limit the administrators allowed to use sudo to those who require the ability to run commands as root.

The computer uses a file named /etc/sudoers to determine which users can use sudo. You can modify root user access by changing the /etc/sudoers file to restrict sudo access to specific accounts, and allow those accounts to perform specifically allowed commands. This gives you control over what users can do as root.

To restrict sudo usage by changing the /etc/sudoers file:

1 As the root user, use the following command to edit the /etc/sudoers file, which allows for safe editing of the file.

```
$ sudo visudo
```

2 When prompted, enter the administrator password.

There is a timeout value associated with `sudo`. This value indicates the number of minutes until `sudo` prompts for a password again. The default value is 5, which means that after issuing the `sudo` command and entering the correct password, additional `sudo` commands can be entered for 5 minutes without reentering the password.

This value is set in the /etc/sudoers file. For more information, see the `sudo` and `sudoers` man pages.

3 In the Defaults specification section of the file, add the following lines.

```
Defaults timestamp_timeout=0
Defaults tty_tickets
```

These lines limit the use of the sudo command to a single command per authentication and also ensure that, even if a timeout is activated, that later `sudo` commands are limited to the terminal in which authentication occurred.

4 Restrict which administrators are allowed to run `sudo` by removing the line that begins with `%admin` and add the following entry for each user, substituting the user's short name for the word *user*:

user `ALL=(ALL) ALL`

Doing this means that when an administrator is added to the computer, the administrator must be added to the /etc/sudoers file as described, if the administrator needs to use `sudo`.

5 Save and quit `visudo`.

For more information, enter `man pico` or `man visudo` in a Terminal window. For information about how to modify the /etc/sudoers file, see the `sudoers` man page.

Understanding Directory Domains

User accounts are stored in a directory domain. Your preferences and account attributes are set according to the information stored in the directory domain.

Local accounts are hosted in a local directory domain. When you log in to a local account, you authenticate with that local directory domain.

Users with local accounts typically have local home folders. When a user saves files in a local home folder, the files are stored locally. To save a file over the network, the user must connect to the network and upload the file.

Network accounts are hosted in a network directory domain, such as a Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) directory. When you log in to a network account, you authenticate with the network directory domain.

Users with network accounts typically have network home folders. When they save files in their network home folders, the files are stored on the server.

Mobile accounts cache authentication information and managed preferences. A user's authentication information is maintained on the directory server but is cached on the local computer. With cached authentication information, a user can log in using the same user name and password (or a digital token, smart card, or biometric reader), even if the user is not connected to the network.

Users with mobile accounts have local and network home folders, which combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders. For information about protecting your home folder, see Chapter 7, "Securing Data and Using Encryption."

Understanding Network Services, Authentication, and Contacts

You can use Directory Utility to configure your computer to use a network directory domain. Directory search services that are not used should be disabled in the Services pane of Directory Utility.

You can enable or disable each kind of directory service protocol in Directory Utility.

Leopard doesn't access disabled directory services, except for the local directory domain, which is always accessed. In addition to enabling and disabling services, you can use Directory Utility to choose the directory domains you want to authenticate with.

Directory Utility defines the authentication search policy that Leopard uses to locate and retrieve user authentication information and other administrative data from directory domains.

The login window, Finder, and other parts of Leopard use this authentication information and administrative data. File service, Mail service, and other services provided by Mac OS X Server also use this information.

Directory Utility also defines the contacts search policy that Leopard uses to locate and retrieve name, address, and other contact information from directory domains. Address Book can use this contact information, and other applications can be programmed to use it as well.

The authentication and contacts search policy consists of a list of directory domains (also known as directory nodes). The order of directory domains in the list defines the search policy.

Starting at the top of the list, Leopard searches each listed directory domain in turn until it finds the information it needs or reaches the end of the list without finding the information.

For more information about using Directory Utility, see *Open Directory Administration*.

Configuring LDAPv3 Access

Leopard primarily uses Open Directory as its network-based directory domain. Open Directory uses LDAPv3 as its connection protocol. LDAPv3 includes several security features that you should enable if your server supports them. Enabling every LDAPv3 security feature maximizes your LDAPv3 security.

To make sure your settings match your network's required settings, contact your network administrator. Whenever possible, all LDAP connections should be configured to be encrypted using SSL.

When configuring LDAPv3, do not add DHCP-supplied LDAP servers to automatic search policies if you cannot secure the network the computer is running on. If you do, someone can create a rogue DHCP server and a rogue LDAP directory and then control your computer as the root user.

For information about changing the security policy for an LDAP connection or about protecting computers from malicious DHCP servers, see *Open Directory Administration*.

Configuring Active Directory Access

Leopard supports mutual authentication with Active Directory servers. Kerberos is a ticket-based system that enables mutual authentication. The server must identify itself by providing a ticket to your computer. This prevents your computer from connecting to rogue servers.

Leopard also supports digital signing and encrypted packet security settings used by Active Directory. These setting are enabled by default.

Mutual authentication occurs when you bind to Active Directory servers.

If you're connecting to an Active Directory server with Highly Secure (HISEC) templates enabled, you can use third-party tools to further secure your Active Directory connection.

When you configure Active Directory access, the settings you choose are generally dictated by the Active Directory server's settings. To make sure your settings match your network's required settings, contact your network administrator.

The "Allow administration by" setting should not be used in sensitive environments. It can cause untended privilege escalation issues because any member of the group specified will have administrator privileges on your computer. Additionally, you should only connect to trusted networks.

For more information about using Directory Utility to connect to Active Directory servers, see *Open Directory Administration*.

Using Strong Authentication

Authentication is the process of verifying the identity of a user. Leopard supports local and network-based authentication to ensure that only users with valid authentication credentials can access the computer's data, applications, and network services.

You can require passwords to log in, to wake the computer from sleep or from a screen saver, to install applications, or to change system settings. Leopard also supports authentication methods such as smart cards, digital tokens, and biometric readers.

Strong authentication is created by using combinations of the following authentication methods:

- What the user knows, such as a password or PIN number
- What the user has, such as SecurID card, smart card, or driver license
- What the user is, such as a fingerprint, retina scan, or DNA sample

Using a combination of these methods makes authentication more reliable and user identification more certain.

Using Password Assistant to Generate or Analyze Passwords

Mac OS X includes Password Assistant, an application that analyzes the complexity of a password or generates a complex password for you. You can specify the length and type of password you'd like to generate.

You can choose from the following types of passwords:

- **Manual:** You enter a password and then Password Assistant gives you the quality level of your password. If the quality level is low, Password Assistant gives tips for increasing the quality level.
- **Memorable:** According to your password length requirements, Password Assistant generates a list of memorable passwords in the Suggestion menu.
- **Letters & Numbers:** According to your password length requirements, Password Assistant generates a list of passwords with a combination of letters and numbers.
- **Numbers Only:** According to your password length requirements, Password Assistant generates a list of passwords containing only numbers.

- **Random:** According to your password length requirements, Password Assistant generates a list of passwords containing random characters.
- **FIPS-181 compliant:** According to your password length requirements, Password Assistant generates a password that is FIPS-181 compliant (which includes mixed upper and lowercase, punctuation, and numbers).

You can open Password Assistant from some applications. For example, when you create an account or change passwords in Accounts preferences, you can use Password Assistant to help you create a secure password.

Using Kerberos

Kerberos is an authentication protocol used for systemwide single sign-on, allowing users to authenticate to multiple services without reentering passwords or sending them over the network. Every system generates its own principals, allowing it to offer secure services that are fully compatible with other Kerberos-based implementations.

Note: Leopard supports Kerberos v5 but does not support Kerberos v4.

Leopard uses Kerberos to make it easier to share services with other computers. A key distribution center (KDC) server is not required to use Kerberos authentication between two computers running Leopard. When you connect to a computer that supports Kerberos, you are granted a ticket that permits you to continue to use services on that computer, without reauthentication, until your ticket expires.

For example, consider two computers running Leopard named Mac01 and Mac02. Mac02 has screen sharing and file sharing turned on. If Mac01 connects to one of the shared folders on Mac02, Mac01 can subsequently connect to screen sharing on "family" without needing to supply login credentials again.

This Kerberos exchange is only attempted if you connect using Bonjour (for example, if you navigate to the computer in Finder, or you use the Go menu in Finder to connect to a server using the local hostname of the computer name).

Normally, after your computer obtains a Kerberos ticket in this manner, keep that Kerberos ticket until it expires. However, if you want to manually remove your Kerberos ticket, you can do so using the Kerberos utility in Leopard.

To manually remove the Kerberos ticket:

1. Open Keychain Access (in /Applications/Utilities).
2. From the Keychain Access menu, choose Kerberos Ticket Viewer.
3. In the Kerberos application Ticket Cache window, find the key that looks like this:

 `"yourusername@LKDC:SHA1…"`

 It is followed by a long string of alphanumeric characters.
4. Click "Destroy" to delete that key.

You can also use the `kinit`, `kdestroy`, and `kpasswd` commands to manage Kerberos tickets. For more information, see `kinit`, `kdestroy`, and `kpasswd` man pages.

Using Smart Cards

A smart card is a plastic card (similar in size to a credit card) or USB dongle that has memory and a microprocessor embedded in it. The smart card can store and process information such as passwords, certificates, and keys.

The microprocessor inside the smart card can complete its own authentication evaluation offline before releasing information.

Before the smart card processes information, you must authenticate with the smart card by a PIN or biometric measurement (such as a fingerprint), which provides an additional layer of security.

For more information, see the *Smart Card Setup Guide* at www.apple.com/itpro/federal/.

Smart card support is integrated into Leopard Server and can be configured to work with the following services:

- Cryptographic login (local or network accounts)
- Unlock of FileVault enabled accounts
- Unlock keychains
- Signed and encrypted email (S/MIME)
- Securing web access (HTTPS)
- VPN (L2TP, PPTP, SSL)
- 802.1X
- Screen saver unlock
- System administration
- Keychain access

For more information, see the *Smart Card Setup Guide* at www.apple.com/server/macosx/resources/.

Using Tokens

Use a digital token to identify a user for commerce, communication, or access control. This token can be generated by software or hardware.

Common tokens are generated by RSA SecurID and the CRYPTOCard KT-1. These hardware devices generate tokens to identify the user. The generated tokens are specific to that user, so two users with different RSA SecurIDs or different CRYPTOCard KT-1s have different tokens.

You can use tokens for *two-factor* authentication. Two-factor refers to authenticating through something you have (a one-time-password token) and something you know (a fixed password). The use of tokens increases the strength of the authentication process. Tokens are frequently used for VPN authentication.

Using Biometrics

Leopard supports biometrics-based authentication technologies such as thumbprint readers. Password-protected websites and applications can now be accessed without requiring the user to remember a long list of passwords.

Some biometric devices allow you to authenticate by placing your finger on a pad. Fingerprint identification provides personal authentication and network access.

The use of biometrics can add an additional factor to authentication by using something that is a part of you (such as your fingerprint).

Setting Global Password Policies

To configure a password policy that can apply globally or to individual users, use the `pwpolicy` command-line tool, but keep in mind that the pwpolicy tool cannot enforce password policy on local administrator accounts.

You can set specific rules governing the size and complexity of acceptable passwords. For example, you can specify requirements for the following:

- Minimum and maximum character length
- Alphabetic and numeric character inclusion
- Maximum number of failed logins before account lockout

For advanced password policies, use Password Server in Leopard Server. You can use it to set global password policies that specify requirements for the following:

- Password expiration duration
- Special character inclusion
- Mixed-case character inclusion
- Password reuse limits

To require that an authenticator's password be a minimum of 12 characters and have no more than 3 failed login attempts, enter the following in a Terminal window, where *authenticator* is the authenticator's name.

```
$ pwpolicy -a authenticator -setpolicy "minChars=12
     maxFailedLoginAttempts=3”
```

Global password policies are not implemented in Leopard; instead, password policies are set for each user account.

You can use `pwpolicy` to set a password policy that meets your organization's password standards. For more information about how to use `pwpolicy`, enter `man pwpolicy` in a Terminal window.

Storing Credentials in Keychains

Leopard includes Keychain Access, an application that manages collections of passwords and certificates in a single credential store called a keychain. Each keychain can hold a collection of credentials and protect them with a single password.

Keychains store encrypted passwords, certificates, and other private values (called secure notes). These values are accessible only by unlocking the keychain using the keychain password and only by applications that are approved and added to the access control application list.

You can create multiple keychains, each of which appears in a keychain list in Keychain Access. Each keychain can store multiple values. Each value is called a key item. You can create a key item in any user-created keychain.

When an application must store an item in a keychain, it stores it in the keychain designated as your default. The default is named "login," but you can change that to any user-created keychain. The default keychain name is displayed in bold.

Each item in a keychain has an ACL that can be populated with applications that have authority to use that keychain item. A further restriction can be added that forces an application with access to confirm the keychain password.

The main issue with remembering passwords is that you're likely to make all passwords identical or keep a written list of passwords. By using keychains, you can greatly reduce the number of passwords you need to remember. Because you no longer need to remember passwords for multiple accounts, the passwords you choose can be very complex and can even be randomly generated.

Keychains provide additional protection for passwords, passphrases, certificates, and other credentials stored on the computer. In some cases, such as using a certificate to sign a mail message, the certificate must be stored in a keychain.

If a credential must be stored on the computer, store and manage it using Keychain Access. Check your organization's policy on keychain use.

Due to the sensitive nature of keychain information, keychains use cryptography to encrypt and decrypt secrets, and they safely store secrets and related data in files.

Leopard Server Keychain services enable you to create keychains and provide secure storage of keychain items. After a keychain is created, you can add, delete, and edit keychain items, such as passwords, keys, certificates, and notes for users. A user can unlock a keychain with a single password and applications can then use that keychain to store and retrieve data, such as passwords.

Note: You can use the `security` command to administer keychains, manipulate keys and certificates, and do just about anything the Security framework can do. For more information about this command, see its man page.

Using the Default User Keychain

When a user's account is created, a default keychain named "login" is created for that user. The password for the login keychain is initially set to the user's login password and is unlocked when the user logs in. It remains unlocked unless the user locks it, or until the user logs out.

You should change the settings for the login keychain so the user must unlock it when he or she logs in, or after waking the computer from sleep.

To secure the login keychain:

1. Open Keychain Access.
2. If you do not see a list of keychains, click Show Keychains.
3. Select the login keychain.
4. Choose Edit > Change Password for Keychain "login."
5. Enter the current password and create and verify a password for the login keychain.

 After you create a login keychain password that is different from the normal login password, your keychain is not unlocked at login.

 To help you create a more secure password, use Password Assistant. For information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.
6. Choose Edit > Change Settings for Keychain "login."
7. Select "Lock when sleeping."
8. Deselect "Synchronize this keychain using MobileMe."
9. Secure each login keychain item.

 For information, see "Securing Keychains and Their Items" on page 110.

Creating Additional Keychains

When a user account is created it contains only the initial default keychain named "login." A user can create additional keychains, each of which can have different settings and purposes.

For example, a user might want to group credentials for mail accounts into one keychain. Because mail programs query the server frequently to check for mail, it is not practical for the user to reauthenticate when such a check is performed.

The user could create a keychain and configure its settings, so that he or she is required to enter the keychain password at login and when the computer is awakened from sleep.

He or she could then move all items containing credentials for mail applications into that keychain and set each item so that only the mail application associated with that credential can access it. This forces other applications to authenticate to access that credential.

Configuring a keychain's settings for use by mail applications might be unacceptable for other applications. If a user has an infrequently used web-based account, it is more appropriate to store keychain settings in a keychain configured to require reauthentication for every access by any application.

You can also create multiple keychains to accommodate varying degrees of sensitivity. By separating keychains based on sensitivity, you prevent the exposure of sensitive credentials to less sensitive applications with credentials on the same keychain.

To create a keychain and customize its authentication settings:

1. In Keychain Access, choose File > New Keychain.
2. Enter a name, select a location for the keychain, and click Create.
3. Enter a password, verify it, and click OK.
4. If you do not see a list of keychains, click Show Keychains.
5. Select the new keychain.
6. Choose Edit > Change Settings for keychain "*keychain_name*," and authenticate, if requested.
7. Change the "Lock after # minutes of inactivity" setting based on the access frequency of the security credentials included in the keychain.

 If the security credentials are accessed frequently, do not select "Lock after # minutes of inactivity."

 If the security credentials are accessed frequently, select "Lock after # minutes of inactivity" and select a value, such as 15. If you use a password-protected screensaver, consider setting this value to the idle time required for your screensaver to start.

 If the security credentials are accessed infrequently, select "Lock after # minutes of inactivity" and specify a value, such as 1.
8. Select "Lock when sleeping."

9 Drag the security credentials from other keychains to the new keychain and authenticate, if requested.

You should have keychains that only contain related certificates. For example, you could have a mail keychain that only contains mail items.

10 If you are asked to confirm access to the keychain, enter the keychain password and click Allow Once.

After confirming access, Keychain Access moves the security credential to the new keychain.

11 Secure each item in the security credentials for your keychain.

For information, see "Securing Keychains and Their Items" on page 110.

Securing Keychains and Their Items

Keychains can store multiple encrypted items. You can configure items so only specific applications have access. (However, you cannot set Access Control for certificates.)

To secure a keychain item:

1 In Keychain Access, select a keychain, and then select an item.

2 Click the Information (i) button.

3 Click Access Control and then authenticate if requested.

4 Select "Confirm before allowing access."

After you enable this option, Leopard prompts you before giving a security credential to an application.

If you selected "Allow all applications to access this item," you allow any application to access the security credential when the keychain is unlocked. When accessing the security credential, there is no user prompt, so enabling this is a security risk.

5 Select "Ask for Keychain password."

After selecting this, you must provide the keychain password before applications can access security credentials.

Enabling this is important for critical items, such as your personal identity (your public key certificates and the corresponding private key), which are needed when signing or decrypting information. These items can also be placed in their own keychains.

6 Remove nontrusted applications listed in "Always allow access by these applications" by selecting each application and clicking the Remove (–) button.

Applications listed here require the user to enter the keychain password to access security credentials.

Using Smart Cards as Keychains

Leopard Server integrates support for hardware based smart cards as dynamic keychains where any application using keychains can access that smart card.

Smart cards are dynamic keychains, are added to the top of the keychain access list, and are the first searched in the list. They can be treated as other keychains on the user's computer, with the limitation of adding other secure objects.

You cannot store passwords or other types of information on your smart card. A smart card can be viewed as a portable protected keychain.

When you attach a supported smart card to your computer, it is displayed in Keychain Access. If multiple smart cards are attached to your computer, they appear at the top of the keychain list alphabetically as separate keychains.

You can manually unlock and change the PIN using Keychain access. When changing the PIN on your smart card, it is the same as changing the password on a regular keychain.

In Keychain Access, select your smart card and unlock it by double-clicking it. If it is not unlocked, you are prompted to enter the password for the smart card, which is the same as the PIN. Enter the PIN and Keychain Access will bring up the PIN-protected data on that smart card.

For more information, see the *Smart Card Setup Guide* at www.apple.com/server/macosx/resources/.

Using Portable and Network Keychains

If you're using a portable computer, consider storing your keychains on a portable drive, such as a USB flash memory drive. You can remove the portable drive from the portable computer and store it separately when the keychains are not in use.

Anyone attempting to access data on the portable computer needs the portable computer, portable drive, and password for the keychain stored on the portable drive. This provides an extra layer of protection if the laptop is stolen or misplaced.

To use a portable drive to store keychains, move your keychain files to the portable drive and configure Keychain Access to use the keychains on the portable drive.

The default location for your keychain is ~/Library/Keychains/. However, you can store keychains in other locations.

You can further protect portable keychains by storing them on biometric USB flash memory drives, or by storing portable drive contents in an encrypted file.
For information, see "Encrypting Portable Files" on page 166.

Check with your organization to see if they allow portable drives to store keychains.

Securing System Preferences

6

Use this chapter to set Leopard Server system preferences to enhance system security and further protect against attacks.

System Preferences has many configurable preferences that you can use to enhance system security. You can also manage these preferences using Workgroup Manager.

System Preferences Overview

Leopard includes system preferences that you can customize to improve security. When modifying settings for one account, make sure your settings are mirrored on all other accounts, unless there is an explicit need for different settings.

You can view system preferences by choosing Apple > System Preferences. In the System Preferences window, click a preference to view it.

Some critical preferences require that you authenticate before you modify their settings. To authenticate, you click the lock (see the images below) and enter an administrator's name and password (or use a digital token, smart card, or biometric reader).





If you log in as a user with administrator privileges, these preferences are unlocked unless you select "Require password to unlock each System Preferences pane" in Security preferences. For more information, see "Securing Security Preferences" on page 138.

If you log in as a standard user, these preferences remain locked. After unlocking preferences, you can lock them again by clicking the lock.

Preferences that require authentication include the following:

- Accounts
- Date & Time
- Energy Saver
- Network
- Print & Fax
- Security
- Sharing
- Startup Disk
- Time Machine

This chapter lists each set of preferences included with Leopard and describes modifications recommended to improve security.

Securing MobileMe Preferences

MobileMe is a suite of Internet tools that help you synchronize data and other important information when you're away from the computer.

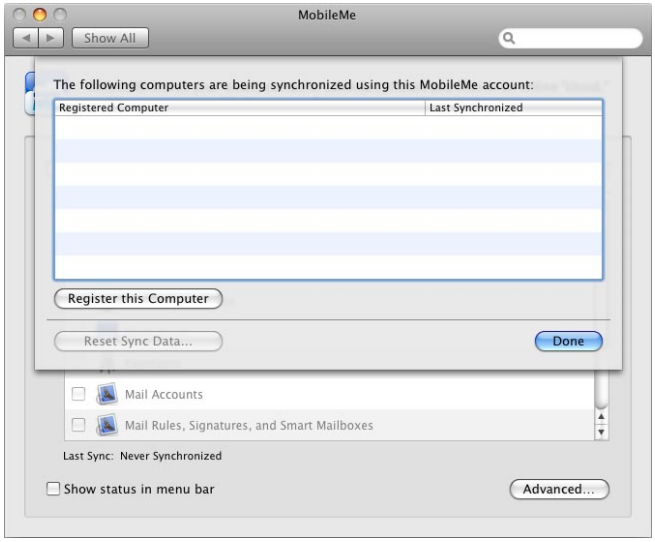
In sensitive environments don't use MobileMe. If you must store critical data, only store it on your local computer. You should only transfer data over a secure network connection to a secure internal server.

If you use MobileMe, enable it only for user accounts that don't have access to critical data. It is not recommended that you enable MobileMe for administrator or root user accounts.

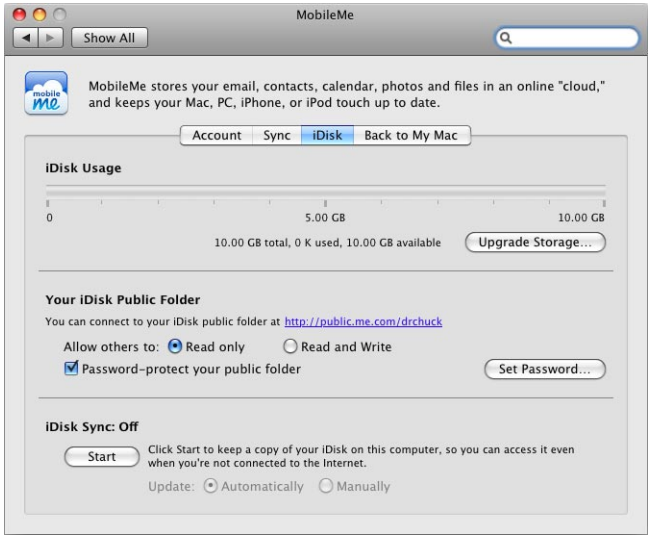
Leave the options disabled in the Sync pane of MobileMe preferences (shown below).



Leave Registered Computer for synchronization blank in the Advanced settings of the Sync pane (shown below).



Leave iDisk Syncing (shown below) disabled by default. If you must use a Public folder, enable password protection.



To disable MobileMe preferences:

1. Open MobileMe preferences.
2. Deselect "Synchronize with MobileMe."

3 Make sure there are no computers registered for synchronization in the Advanced settings of the Sync pane.

4 Make sure iDisk Syncing is disabled in the iDisk pane.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing System Preferences
# ------------------------------------------------------------------
# Securing MobileMe Preferences
# ------------------------
# Disable Sync options.
defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer 1
# Disable iDisk Syncing.
defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool no
```

Securing Accounts Preferences

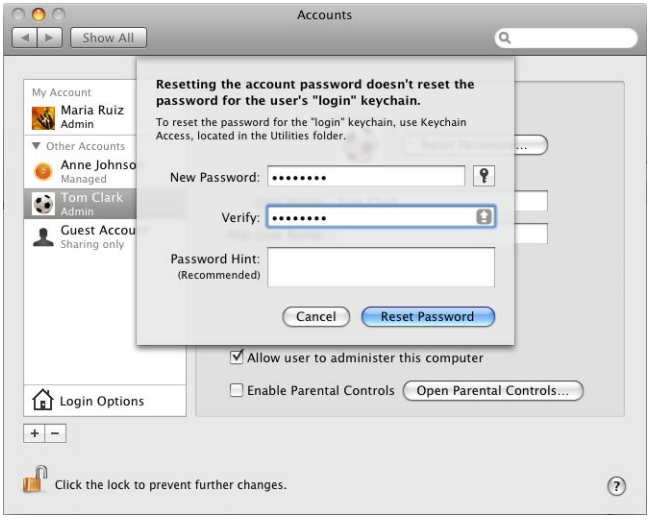
Use Accounts preferences to change or reset account passwords (shown below), to enable Parental Controls, or to modify login options for each account.

You should immediately change the password of the first account that was created on your computer. If you are an administrator, you can change other user account passwords by selecting the account and clicking Change Password.

Note: If you are an administrator, password policies are not enforced when you change your password or when you change another user's password. Therefore, when you are changing passwords as an administrator, make sure you follow the password policy you set. For more information about password policies, see "Setting Global Password Policies" on page 106.



The password change dialog (shown below) and the reset dialog provide access to Password Assistant, an application that can analyze the strength of your chosen password and assist you in creating a more secure password. For information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.



Consider the following login guidelines:

- Modify login options to provide as little information as possible to the user.
- Require that the user know which account they want to log in with, and the password for that account.
- Don't automatically log the user in.
- Require that the user enter a name and a password, and that the user authenticate without the use of a password hint.
- Don't enable fast user switching—it is a security risk because it allows multiple local users to be simultaneously logged in to a computer.

You should also modify login options to disable the Restart, Sleep, and Shut Down buttons. By disabling these buttons, the user cannot restart the computer without pressing the power key or logging in.

To securely configure Accounts preferences:

1. Open Accounts preferences.
2. Select an account and click the Password tab; then change the password by clicking the Change Password button.

 A menu appears asking you to input the old password, new password, verification of the new password, and a password hint.
3. Do not enter a password hint, then click the Change Password button.
4. Click Login Options.

 A screen similar to the following appears:



5 Under "Display login window as" select "Name and password" and deselect all other options.

From the Command Line:

```
# Securing Accounts Preferences
# ----------------------------
# Change an account's password on a client system.
# Don't use this commands if other users are also logged in
sudo dscl /LDAPv3/127.0.0.1 passwd /Users/$User_name $Oldpass $Newpass

# Change an account's password on a server.
# Don't use this commands if other users are also logged in
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass

# Make sure there is no password hint set.
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint
     -int 0

# Set the login options to display name and password in the login window.
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -
     bool yes

# Disable Show the Restart, Sleep, and ShutDown Buttons.
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
     bool yes

# Disable fast user switching. This command does not prevent multiple users
# from being logged in.
defaults write /Library/Preferences/.GlobalPreferences
     MultipleSessionEnabled -bool NO
```

Securing Appearance Preferences

One method to secure appearance preferences is to change the number of recent items displayed in the Apple menu to None.

Recent items are applications, documents, and servers that you've recently used. You can access recent items by choosing Apple > Recent Items.

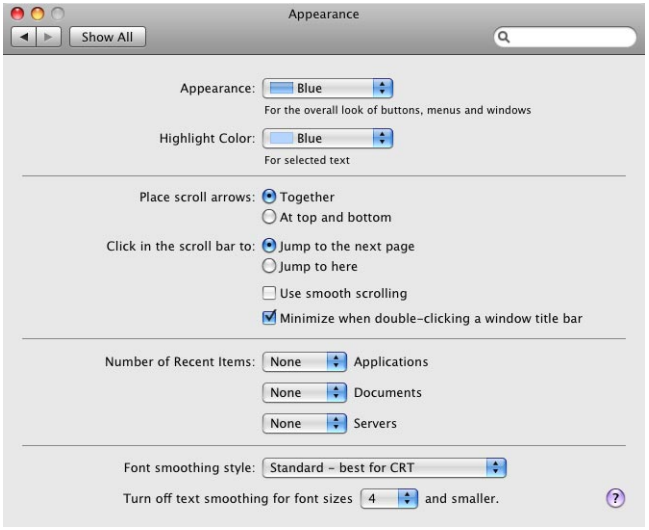
If intruders gain access to your computer, they can use recent items to quickly view your most recently accessed files. Additionally, intruders can use recent items to access authentication mechanisms for servers if the corresponding keychains are unlocked.

Removing recent items provides a minimal increase in security, but it can deter very unsophisticated intruders.

To securely configure Appearance preferences:

1 Open Appearance preferences.

A screen similar to the following appears:



2 Set all "Number of Recent Items" preferences to None.

From the Command Line:

```
# Securing Appearance Preferences
# ------------------------------
# Disable display of recent applications.
defaults write com.apple.recentitems Applications -dict MaxAmount 0
```

Securing Bluetooth Preferences

Bluetooth allows wireless devices, such as keyboards, mice, and mobile phones, to communicate with the computer. If the computer has Bluetooth capability, Bluetooth preferences become available. If you don't see Bluetooth preferences, you cannot use Bluetooth.

Note: Some high security areas do not allow radio frequency (RF) communication such as Bluetooth. Consult your organizational requirements for possible further disablement of the component.

When you disable Bluetooth in System Preferences, you must disable Bluetooth for every user account on the computer.

This does not prevent users from reenabling Bluetooth. You can restrict a user account's privileges so the user cannot reenable Bluetooth, but to do this, you remove several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 94.

Note: To remove Bluetooth support for peripherals, see "Removing Bluetooth Support Software" on page 78.

To securely configure Bluetooth preferences:

1 Open Bluetooth preferences.

A screen similar to the following appears:



2 Deselect "Bluetooth Power."

From the Command Line:

```
# Securing Bluetooth Preferences
# ------------------------------
# Turn Bluetooth off
defaults write /Library/Preferences/com.apple.Bluetooth
     ControllerPowerState -int 0
```

Securing CDs & DVDs Preferences

To secure CDs and DVDs, do not allow the computer to perform automatic actions when the user inserts a disc.

When you disable automatic actions in System Preferences, you must disable these actions for every user account on the computer.

This does not prevent users from reenabling automatic actions. To prevent the user from reenabling automatic actions, you must restrict the user's account so the user cannot open System Preferences. For more information on restricting accounts, see "Securing Nonadministrator Accounts" on page 97.

To securely configure CDs & DVDs preferences:

1 Open CDs & DVDs preferences.

A screen similar to the following appears:



2 Disable automatic actions when inserting media by choosing Ignore for each pop-up menu.

From the Command Line:

```
# Securing CDs & DVDs Preferences
# ------------------------------
# Disable blank CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.cd.appeared -dict action 1

# Disable music CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.music.appeared -dict action 1

# Disable picture CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.picture.appeared -dict action 1

# Disable blank DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.dvd.appeared -dict action 1

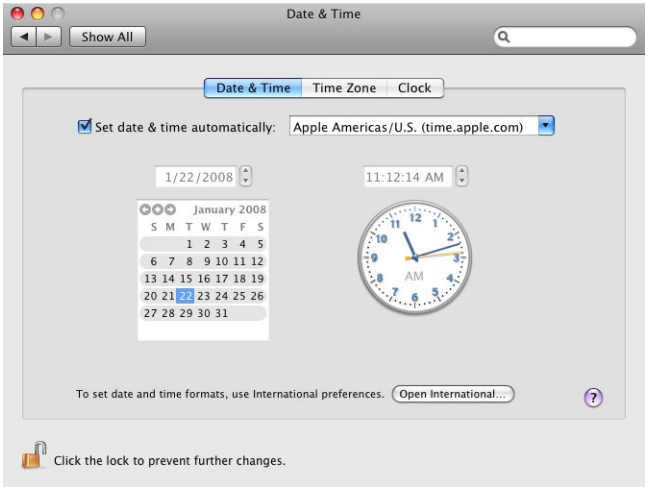
# Disable video DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.dvd.video.appeared -dict action 1
```

Securing Date & Time Preferences

Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues.

You can use Date & Time preferences (shown below) to set the date and time based on a Network Time Protocol (NTP) server.

If you require automatic date and time, use a trusted, internal NTP server.



To securely configure Date & Time preferences:

1. Open Date & Time preferences.
2. In the Date & Time pane, enter a secure and trusted NTP server in the "Set date & time automatically" field.
3. Click the Time Zone button.

A screen similar to the following appears:



4 Choose a time zone.

From the Command Line:

```
# Securing Date & Time Preferences
# --------------------------------
# Set the NTP server.
cat >> /etc/ntp.conf << END server time.apple.com END

# Set the Date and Time.
systemsetup -settimezone $Time_Zone

# Disable NTPD if there is no trusted NTPD available.
launchctl unload -w org.ntp.ntpd.plist
```

Securing Desktop & Screen Saver Preferences

You can use Desktop & Screen Saver preferences (shown below) to configure a password-protected screen saver to prevent unauthorized users from accessing unattended computers.

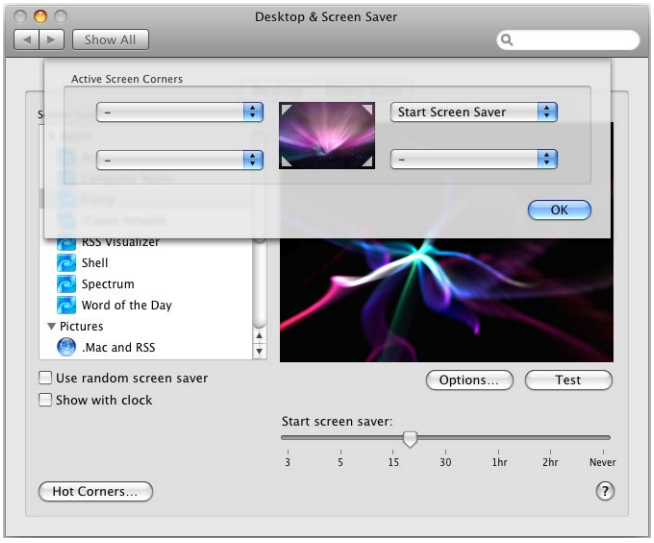


You can use several authentication methods to unlock the screen saver, including digital tokens, smart cards, and biometric readers.

You should also set a short inactivity interval to decrease the amount of time the unattended computer is unlocked. For information about requiring authentication for screen savers, see "Securing Security Preferences" on page 138.

You can configure Desktop & Screen Saver preferences to allow you to quickly enable or disable screen savers if you move your mouse cursor to a corner of the screen, as shown below. (You can also do this by configuring Exposé & Spaces preferences.)

By default, any admin can unlock any user's display.



When you configure Desktop & Screen Saver preferences, you configure the preferences for every user account on the computer.

This doesn't prevent users from reconfiguring their preferences. You can restrict a user's account privileges so the user cannot reconfigure preferences. Doing this removes several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 94.

To securely configure Desktop & Screen Saver preferences:

1. Open Desktop & Screen Saver preferences.
2. Click the Screen Saver pane.
3. Set "Start screen saver" to a short inactivity time.
4. Click Hot Corners.
5. Set a corner to Start Screen Saver for quick enabling of the screen saver, but don't set a screen corner to Disable Screen Saver.

From the Command Line:

```
# Securing Desktop & Screen Saver Preferences
# ----------------------------------------
# Set idle time for screen saver. XX is the idle time in seconds.
defaults -currentHost write com.apple.screensaver idleTime -int XX

# Set host corner to activate screen saver.
# wvous-bl-corner (bottom-left)
# wvous-br-corner(bottom-right)
# wvous-tl-corner (top-left)
# wvous-tr-corner (top-right)
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-corner
     -int 5

# Set modifier key to 0 wvous-corner_code-modifier
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
     modifier -int 0
```

Securing Display Preferences

If you have multiple displays attached to your computer, be aware that enabling display mirroring might expose private data to others. Having this additional display provides extra opportunity for others to see private data.

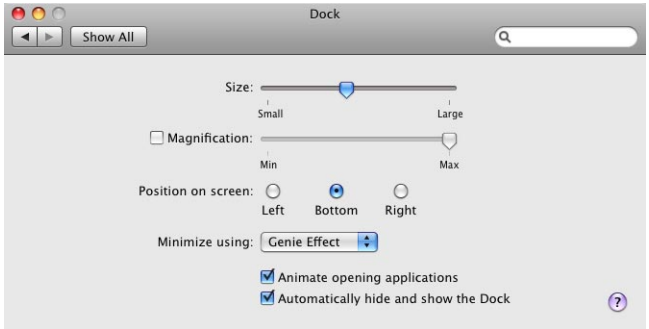
Securing Dock Preferences

You can configure the Dock to be hidden when not in use. This can prevent others from seeing the applications on your computer.

To securely configure Dock preferences:

1 Open Dock preferences.

The following screen appears:



2 Select "Automatically hide and show the Dock."

From the Command Line:

```
# Securing Dock Preferences
# ------------------------
# Automatically hide and show Dock
defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Restart dock
killall -HUP Dock
```

Securing Energy Saver Preferences

You can use Energy Saver Sleep preferences (shown below) to configure a period of inactivity before a computer, display, or hard disk enters sleep mode.

If the computer receives directory services from a network that manages its client computers, when the computer is in sleep mode, it is unmanaged and cannot be detected as being connected to the network. To allow management and network visibility, configure the display and the hard disk to sleep, but not the computer.

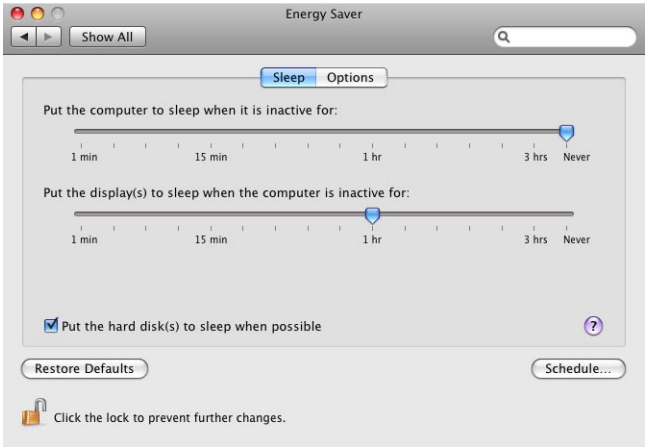
You can require authentication by use of a password, digital token, smart card, or biometric reader to reactivate the computer (see "Securing Security Preferences" on page 138). This is similar to using a password-protected screen saver.

You can also use the Options pane (shown below) to make settings depending on your power supply (power adapter, UPS, or battery). Configure the computer so it only wakes when you physically access the computer. Also, don't set the computer to restart after a power failure.

To securely configure Energy Saver preferences:

1 Open Energy Saver preferences.

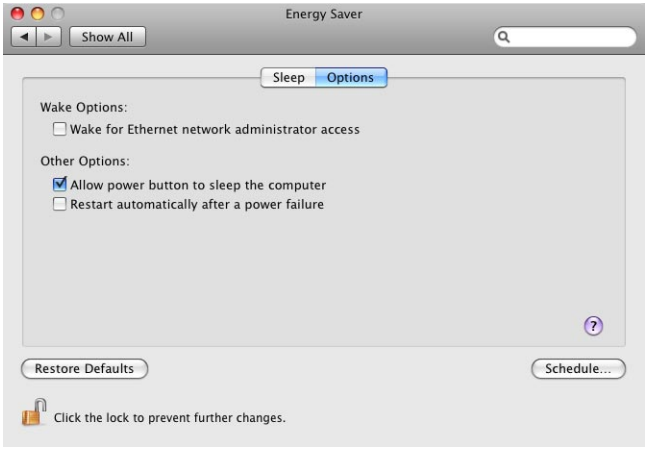
A screen similar to the following appears:



2 From the Sleep pane, set "Put the computer to sleep when it is inactive for" to Never.

3 Select "Put the hard disk(s) to sleep when possible" and then click the "Options" pane.

A screen similar to the following appears:



4 Deselect "Wake for Ethernet network administrator access" and "Restart automatically after a power failure."

From the Command Line:

```
# Securing Energy Saver Preferences
# --------------------------------
# Disable computer sleep.
pmset -a sleep 0

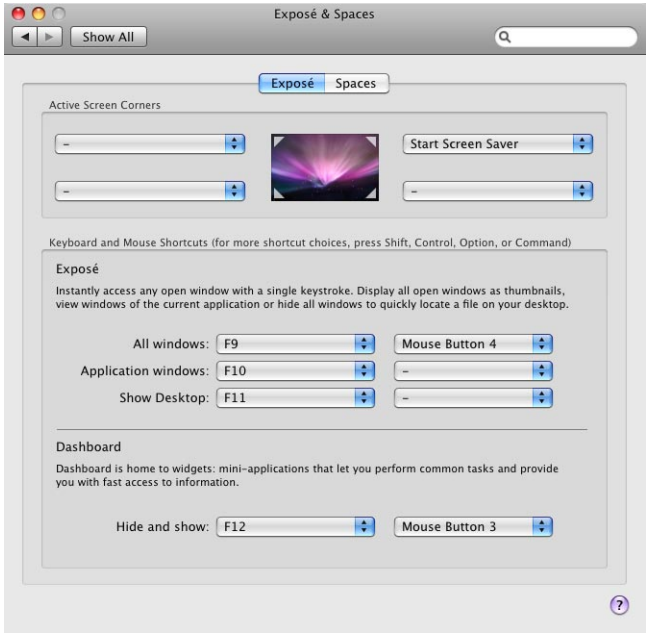
# Enable hard drive sleep.
pmset -a disksleep $minutes

# Disable Wake for Ethernet network administrator access.
pmset -a womp 0

# Disable Restart automatically after power failure.
pmset -a autorestart 0
```

Securing Exposé & Spaces Preferences

Your computer should require authentication when waking from sleep or screen saver. You can configure Exposé & Spaces preferences (shown below) to allow you to quickly start the screen saver if you move your mouse cursor to a corner of the screen, but don't configure a corner to disable the screen saver.



For information about requiring authentication for the screen saver, see “Securing Security Preferences” on page 138.

Dashboard widgets included with Leopard can be trusted. However, be careful when you install third-party Dashboard widgets. You can install Dashboard widgets without authenticating. To prevent Dashboard from running remove the Dashboard application from the /Applications folder.

When you configure Exposé & Spaces preferences, you must configure these preferences for every user account on the computer.

This doesn’t prevent users from reconfiguring their preferences. You can restrict a user account’s privileges so the user cannot reconfigure preferences. To do this, you remove several important user abilities, like the user’s ability to change his or her password. For more information, see “Types of User Accounts” on page 94.

If your organization does not want to use Dashboard because of its potential security risk, you can disable it. If the user has access to the Terminal application, Dashboard can be re-enabled at any time.

Dashboard uses the com.apple.dashboard.fetch service to fetch updates to widgets from the Internet. If Dashboard is disabled, this service should be disabled as well. This service must be disabled from the command line, using the command shown in the instructions below.

From the Command Line:

```
# Securing Exposé & Spaces Preferences
# ------------------------------------
# Disable dashboard.
$ sudo launchctl unload -w /System/Library/LaunchDaemons/
     com.apple.dashboard.advisory.fetch.plist
```

Securing International Preferences

No security-related configuration is necessary. However, if your computer uses more than one language, review the security risk of the language character set. Consider deselecting unused packages during Leopard installation.

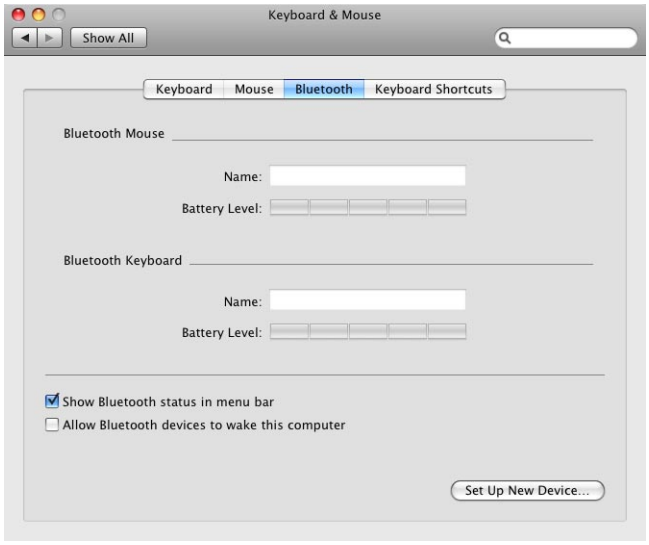
Securing Keyboard & Mouse Preferences

If Bluetooth is not required, turn it off. If Bluetooth is necessary, disable allowing Bluetooth devices to wake the computer.

To securely configure Keyboard & Mouse preferences:

1. Open Keyboard & Mouse preferences.
2. Click Bluetooth.

 A screen similar to the following appears.



3. Deselect "Allow Bluetooth devices to wake this computer."

From the Command Line:

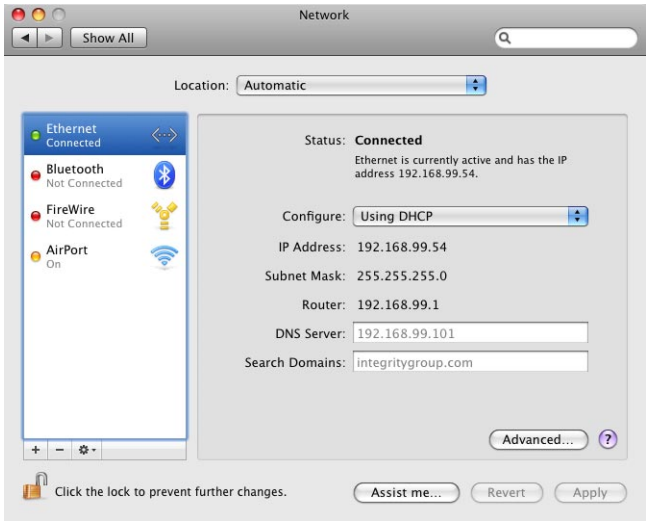
```
# Securing Keyboard & Mouse Preferences
# -------------------------------------
# Disable Bluetooth Devices to wake computer
defaults write /Library/Preferences/com.apple.Bluetooth.plist
     BluetoothSystemWakeEnable -bool 0
```

Securing Network Preferences

To secure Network preferences, disable unused hardware devices listed in Network preferences and IPv6. You should also use a static IP address when possible. A DHCP IP address should be used only if necessary.

Disabling Unused Hardware Devices

Disable unused hardware devices listed in Network preferences (shown below). Enabled, unused devices (such as AirPort and Bluetooth) are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.



To disable unused hardware devices:

1. Open Network Preferences.
2. Click each unused hardware device and choose Off from the Configure pop-up menu.

From the Command Line:

```
# Securing Network Preferences
# ----------------------------
# Disable unused hardware
# The interface value ($interface) can be AirPort, Bluetooth,
“ “Built-in Ethernet”, or “Built-in FireWire”.
networksetup -setnetworkserviceenabled $interface off
```

Disabling IPv6

Some organizations use IPv6, a new version of the Internet protocol (IP). The primary advantage of IPv6 is that it increases the address size from 32 bits (the current IPv4 standard) to 128 bits.

An address size of 128 bits is large enough to support a huge number of addresses, even with the inefficiency of address assignment. This allows more addresses or nodes than are otherwise available. IPv6 also provides more ways to set up the address and simplifies autoconfiguration.

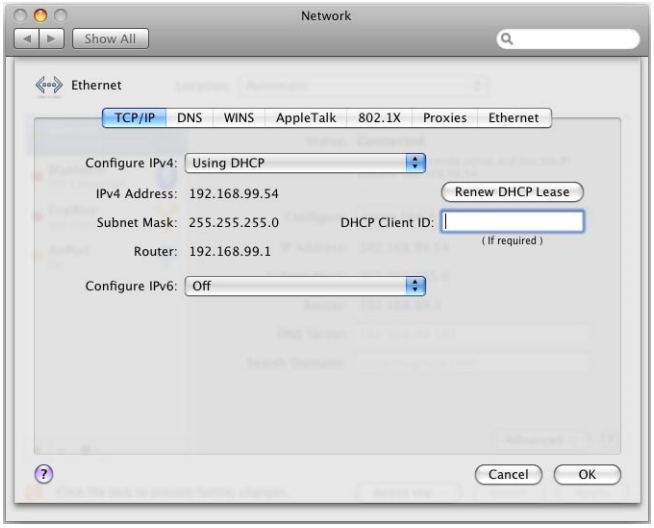
By default IPv6 is configured automatically, and the default settings are sufficient for most computers that use IPv6. You can also configure IPv6 manually. If your organization's network cannot use or does not require IPv6, turn it off.

To disable IPv6 in Network preferences:

1. Open Network preferences.
2. From the list of hardware devices, select the hardware device you use to connect to your network (for example, Airport or Ethernet).

 If you frequently switch between the two, you can disable IPv6 for AirPort and Ethernet or any hardware device that you use to connect to your network.
3. Click Advanced.

 A screen similar to the following appears:



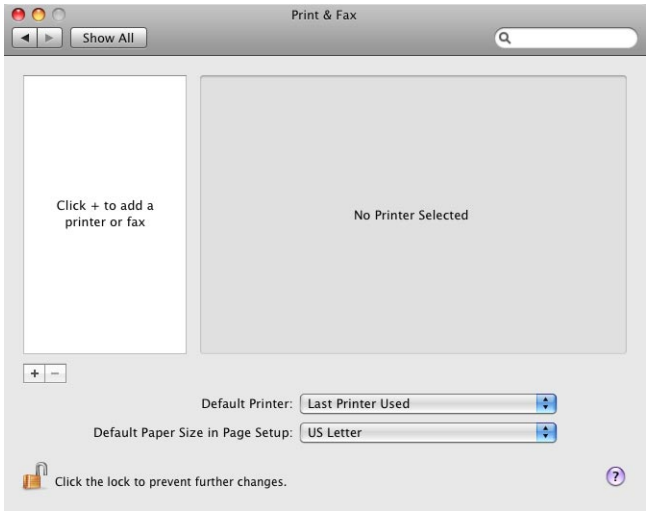
4. In the Configure IPv6 pop-up menu, choose Off.
5. Click OK.

From the Command Line:

```
# Securing Network Preferences
# ----------------------------
# Disable IPv6
# The interface value ($interface) can be AirPort, Bluetooth,
" "Built-in Ethernet", or "Built-in FireWire".
networksetup -setv6off $interface
```

Securing Print & Fax Preferences

The Print & Fax preferences screen looks like this:



Use printers only in a secure location. If you print confidential material in an insecure location, the material might be viewed by unauthorized users.

Be careful when printing to a shared printer. Doing so allows other computers to capture the print job directly. Another computer could be maliciously monitoring and capturing confidential data being sent to the real printer. In addition, unauthorized users can add items to your print queue without authenticating.

Your printer can be accessed using the CUPS web interface (http://localhost:631). By default:

- The CUPS web interface cannot be accessed remotely. It can only be accessed by the local host.
- The titles of all print jobs are available to all users of the system.
- The titles of all print jobs are available to everyone with access to the CUPS web interface.

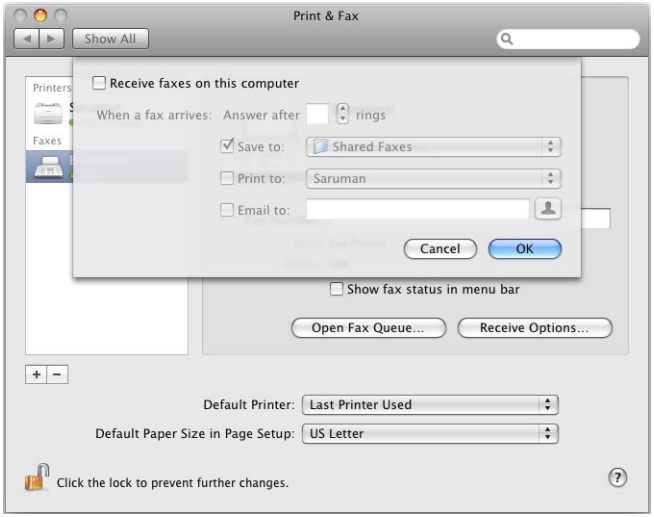
CUPS also offers the ability to browse the network for available printers. Manually specifying available printers is more secure. You can create policies in CUPS that restrict users from such actions as canceling jobs or deleting printers using the CUPS web interface. For more information about creating CUPS policies, see http://localhost:631/help/policies.html.

To avoid an additional avenue of attack, don't receive faxes on your computer.

To securely configure Print & Fax preferences:

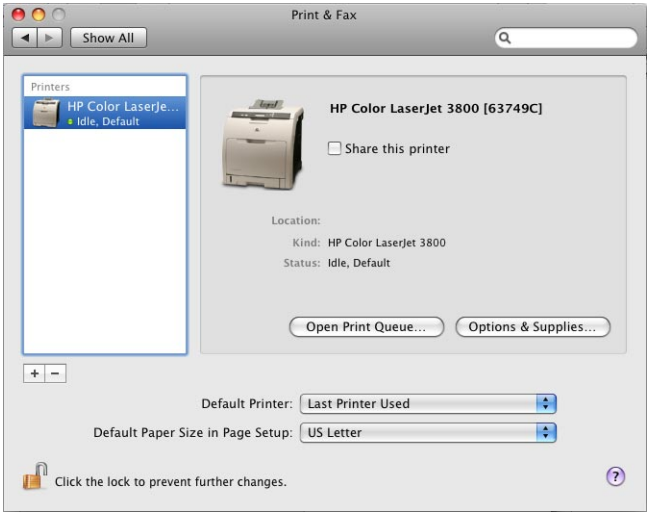
1. Open Print & Fax preferences and select a fax from the equipment list.
2. Click Receive Options.

 A screen similar to the following appears:



3. Deselect "Receive faxes on this computer."
4. Click OK.
5. Select a printer from the equipment list.

 A screen similar to the following appears:



6 Deselect "Share this printer."

From the Command Line:

```
# Securing Printer & Fax Preferences
# ---------------------------------
# Disable the receiving of faxes.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist

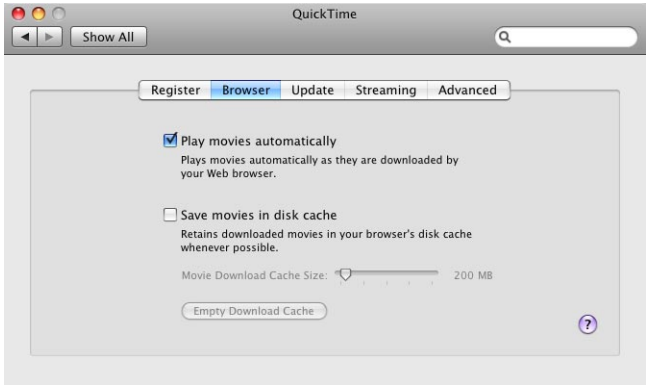
# Disable printer sharing.
cp /etc/cups/cupsd.conf $TEMP_FILE
if /usr/bin/grep "Port 631" /etc/cups/cupsd.conf
then
     /usr/bin/sed "/^Port 631.*/s//Listen localhost:631/g" $TEMP_FILE
     /etc/cups/cupsd.conf
else
     echo "Printer Sharing not on"
fi

# Disable printer browsing
Browsing Off
BrowseAllow none
```

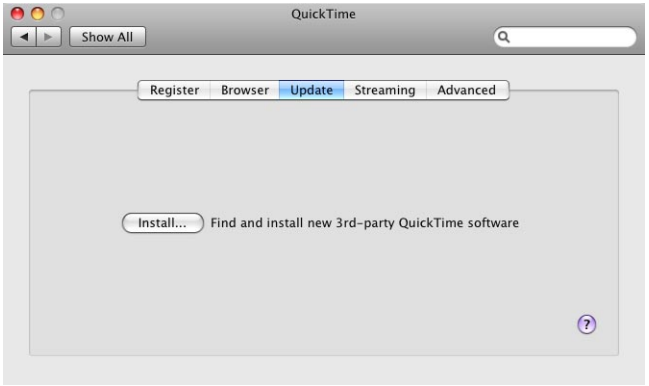
Securing QuickTime Preferences

Download QuickTime movies from trusted, secure sources only. By default, QuickTime stores downloaded movies in a cache. If someone gains access to your account they can see your previously viewed movies, even if you did not save them as files.

You can change QuickTime preferences to disable the storing of movies in a cache (in /Users/*user name*/Library/Caches/QuickTime/downloads/), as shown here.



You can find and install third-party QuickTime software using the Update pane (shown below). Install third-party QuickTime software only if your organization requires that software.



To securely configure QuickTime preferences:

1. Open QuickTime preferences.
2. In the Browser pane, deselect "Save movies in disk cache."

Securing Security Preferences

The settings in Security preferences (shown here) cover a range of Leopard Server security features, including login options, FileVault, and firewall protection.



To securely configure Security preferences:

1. Open Security preferences.
2. In the General pane, select the following:
 - "Require password to wake this computer from sleep or screen saver"
3. In the FileVault pane, select "Turn on FileVault."
4. Authenticate with your account password.
5. Select "Use secure erase" and click "Turn on FileVault."
6. Restart the computer.

From the Command Line:

```
# Securing Security Preferences
# ----------------------------
# Enable Require password to wake this computer from sleep or screen
# saver.
defaults -currentHost write com.apple.screensaver askForPassword -int 1

# Enable FileVault.
# To enable FileVault for new users, use this command.
/System/Library/CoreServices/ManagedClient.app/Contents/Resources/
     createmobileaccount
```

Securing Sharing Preferences

By default, every service listed in Sharing preferences is disabled except for remote login (SSH). Do not enable these services unless you use them. The following services are described in detail in *Mac OS X Security Configuration*.

Service	Description
DVD or CD Sharing	Allows users of other computers to remotely use the DVD or CD drive on your computer.
Screen Sharing	Allows users of other computers to remotely view and control the computer.
File Sharing	Gives users of other computers access to each user's Public folder.
Printer Sharing	Allows other computers to access a printer connected to this computer.
Web Sharing	Allows a network user to view web sites located in /Sites. If you enable this service, securely configure the Apache web server.
Remote Login	Allows users to access the computer remotely by using SSH. If you require the ability to perform remote login, SSH is more secure than telnet, which is disabled by default.
Remote Management	Allows the computer to be accessed using Apple Remote Desktop.
Remote Apple Events	Allows the computer to receive Apple events from other computers.

Service	Description
Xgrid Sharing	Allows computers on a network to work together in a grid to process a job.
Internet Sharing	Allows other users to connect with computers on your local network, through your internet connection.
Bluetooth Sharing	Allows other Bluetooth-enabled computers and devices to share files with your computer.

You can change your computer's name in Sharing preferences, shown here.



By default your computer's host name is typically *firstname-lastname-computer*, where *firstname* and *lastname* are the system administrator's first name and last name, respectively, and *computer* is the type of computer or "Computer."

When users use Bonjour to discover available services, your computer appears as *hostname*.local. To increase privacy, change your computer's host name so you are not identified as the owner of your computer.

For more information about these services and the firewall and sharing capabilities of Leopard, see *Mac OS X Security Configuration*.

To securely configure Sharing preferences:

1. Open Sharing preferences.
2. Change the default computer name to a name that does not identify you as the owner.

From the Command Line:

```
# Securing Sharing Preferences
# ---------------------------
# Change the computer name, where $host_name is the name of the computer.
# This command does not change the Bonjour host name.
systemsetup -setcomputername $host_name

# Change the Bonjour host name, where $Bon_host_name must not contain
# spaces or other non-DNS characters.
scutil --set LocalHostName $Bon_host_name
```

Securing Software Update Preferences

Your Software Update preferences configuration depends on your organization's policy. For example, if your computer is connected to a managed network, the management settings determine what software update server to use.

Instead of using Software Update (shown here), you can also update your computer by using installer packages.



You could install and verify updates on a test computer before installing them on your operational computer. For more information about how to manually update your computer, see "Updating Manually from Installer Packages" on page 71.

After transferring installer packages to your computer, verify the authenticity of the installer packages. For more information, see "Using Disk Utility to Repair Disk Permissions" on page 74.

When you install a software update using Software Update or an installer package, you must authenticate with an administrator's name and password. This reduces the chance of accidental or malicious installation of software updates.

Software Update will not install a software package that has not been digitally signed by Apple.

To disable automated Software Updates:

1. Open Software Update preferences.
2. Click the Scheduled Check pane.
3. Deselect "Download important updates automatically" and "Check for updates."

From the Command Line:

```
# Securing Software Updates Preferences
# -------------------------------------
# Disable check for updates and Download important updates automatically
softwareupdate --schedule off
```

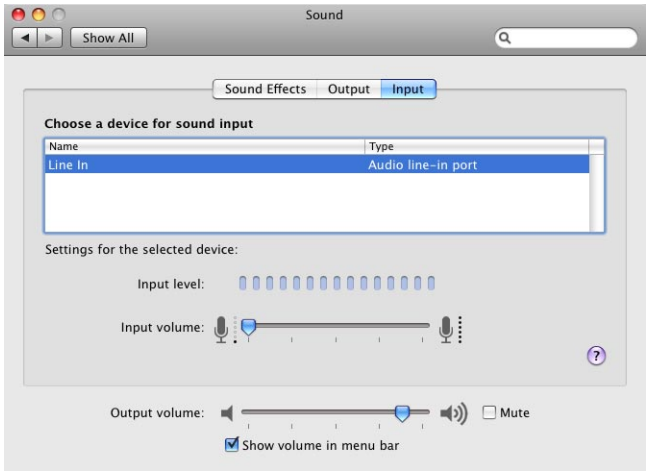
Securing Sound Preferences

Many Apple computers include an internal microphone. You can use Sound preferences (shown below) to disable the internal microphone and the line-in port.

To securely configure Sound preferences:

1. Open Sound preferences.

 A screen similar to the following appears:



2. Select Internal microphone (if present), and set "Input volume" to zero.
3. Select Line-In (if present), and set "Input volume" to zero.

This ensures that “Line-In” is the device selected rather than the internal microphone when Sound preferences is closed. This provides protection from inadvertent use of the internal microphone.

From the Command Line:

```
# Securing Sound Preferences
# -------------------------
# Disable internal microphone or line-in.
# This command does not change the input volume for all input devices. It
# only sets the default input device volume to zero.
osascript -e “set volume input volume 0”
```

Securing Speech Preferences

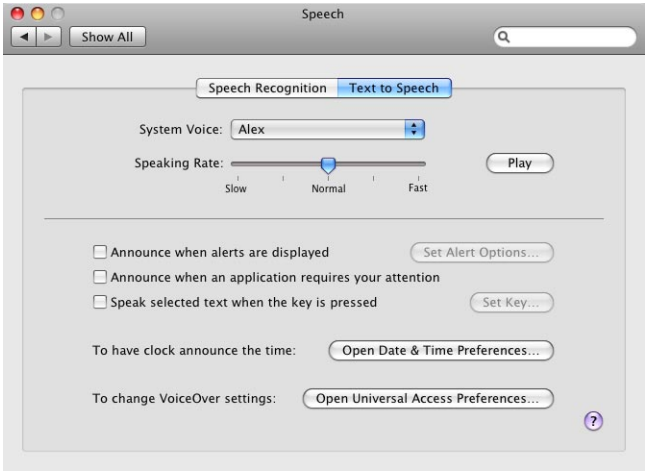
Leopard includes speech recognition and text-to-speech features, which are disabled by default.

Enable these features only if you work in a secure environment where no one can hear you speak to the computer, or hear the computer speak to you. Also make sure no audio recording devices can record your communication with the computer.

The following shows the Speech Recognition preferences pane:



The following shows the Text to Speech pane:



If you enable text-to-speech, use headphones to keep others from overhearing your computer.

To securely configure Speech preferences:

1. Open Speech preferences.
2. Click the Speech Recognition pane and set Speakable Items On or Off.

 Change the setting according to your environment.
3. Click the Text to Speech pane and change the settings according to your environment.

From the Command Line:

```
# Securing Speech Preferences
# ---------------------------
# Disable Speech Recognition
defaults write "com.apple.speech.recognition.AppleSpeechRecognition.prefs"
     StartSpeakableItems -bool false

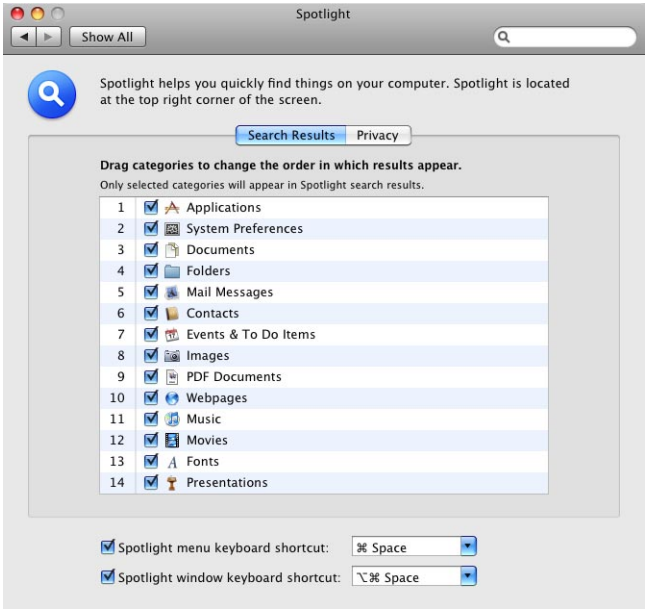
# Disable Text to Speech settings
defaults write "com.apple.speech.synthesis.general.prefs"
     TalkingAlertsSpeakTextFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenNotificationAppActivationFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenUIUseSpeakingHotKeyFlag -bool false
defaults delete "com.apple.speech.synthesis.general.prefs"
     TimeAnnouncementPrefs
```

Securing Spotlight Preferences

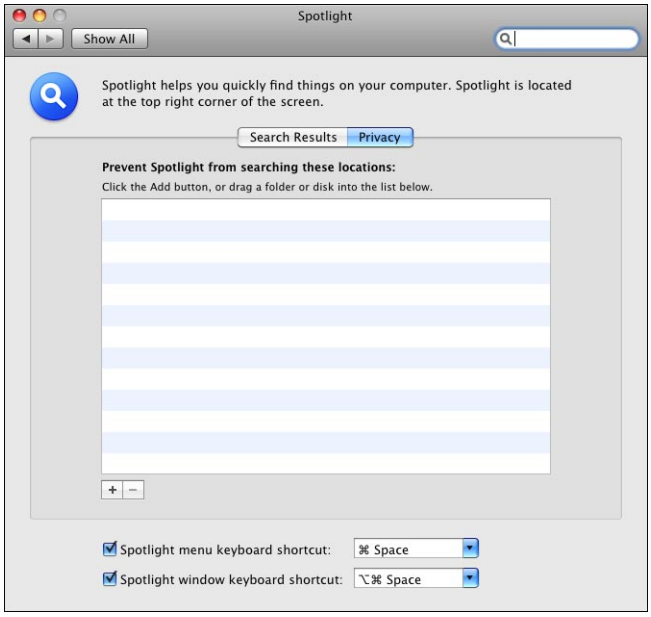
You can use Spotlight to search your computer for files. Spotlight searches the name and meta-information associated with each file and the contents of each file.

Spotlight finds files regardless of their placement in the file system. You must still properly set access permissions on folders containing confidential files. For more information about access permissions, see “Using Disk Utility to Repair Disk Permissions” on page 74.

The Spotlight Preferences Search Results pane appears:



By placing specific folders or disks in the Privacy pane, you can prevent Spotlight from searching them.



Disable the searching of folders that contain confidential information. Consider disabling top-level folders. For example, if you store confidential documents in subfolders of ~/Documents/, instead of disabling each folder, disable ~/Documents/.

By default, the entire system is available for searching using Spotlight.

To securely configure Spotlight preferences:

1. Open Spotlight preferences.
2. In the Search Results pane, deselect categories you don't want searchable by Spotlight.
3. Click the Privacy pane.
4. Click the Add button, or drag a folder or disk into the Privacy pane.

 Folders and disks in the Privacy pane are not searchable by Spotlight.

Note: To prevent users from reenabling Spotlight, remove the rights to access the .Spotlight-V100 folder at the root level of your drive (/.Spotlight-V100/).

From the Command Line:

```
# Securing Spotlight Preferences
# ------------------------------
# Disable Spotlight for a volume and erase its current meta data. Where
# $volumename is the name of the volume.
$ mdutil -E -i off $volumename
```

For more information, enter `man mdutil` in a Terminal window.

Securing Startup Disk Preferences

You can use Startup Disk preferences (shown below) to make your computer start up from a CD, a network volume, a different disk or disk partition, or another operating system.



Be careful when selecting a startup volume:

- Choosing a network install image reinstalls your operating system and might erase the contents of your hard disk.
- If you choose a FireWire volume, your computer starts up from the FireWire disk plugged into the current FireWire port for that volume. If you connect a different FireWire disk to that FireWire port, your computer starts from the first valid Leopard volume available to the computer (if you have not enabled the Open Firmware password).
- When you enable a firmware password, the FireWire volume you select is the only volume that can start the computer. Open Firmware locks the FireWire Bridge Chip GUID as a startup volume instead of the hard disk's GUID (as is done with internal hard disks). If the disk inside the FireWire drive enclosure is replaced by a new disk, the computer can start from the new disk without using the Open Firmware password. To avoid this intrusion make sure your hardware is physically secured. Open Firmware can also have a list of FireWire volumes that are approved for system startup. For information about physically protecting your computer, see "Protecting Hardware" on page 75.

In addition to choosing a new startup volume from Startup Disk preferences, you can restart in Target Disk Mode. When your computer is in Target Disk Mode, another computer can connect to your computer and access your computer's hard disk. The other computer has full access to all files on your computer. All file permissions for your computer are disabled in Target Disk Mode.

To enter Target Disk Mode, hold down the T key during startup. You can prevent the startup shortcut for Target Disk Mode by enabling an Open Firmware or EFI password. If you enable an Open Firmware or EFI password, you can still restart in Target Disk Mode using Startup Disk preferences.

For more information about enabling an Open Firmware or EFI password, see "Using the Firmware Password Utility" on page 87.

To select a Startup Disk:

1. Open Startup Disk preferences.
2. Select a volume to use to start up your computer.
3. Click the "Restart" button to restart from the selected volume.

From the Command Line:

```
# Securing Startup Disk Preferences
# -----------------------------
# Set startup disk
systemsetup -setstartupdisk $path
```

Securing Time Machine Preferences

Time Machine (shown below) makes an up-to-date copy of everything on your Mac—digital photos, music, movies, downloaded TV shows, and documents—and lets you easily go back in time to recover files. Time Machine is off by default.

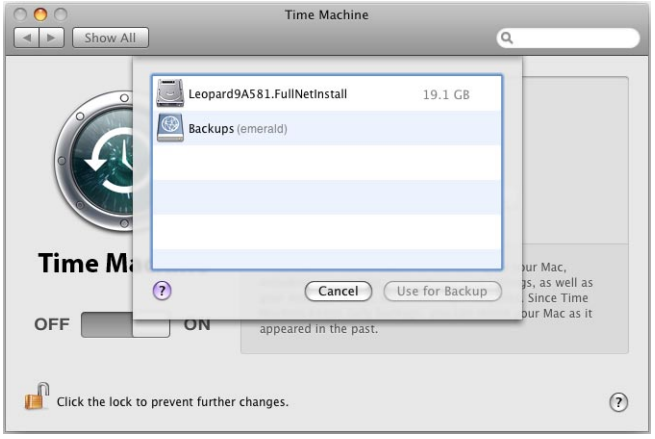
Information stored on your backup disk is not encrypted and can be read by other computers that are connected to your backup disk. Keep your backup disk in a physically secure location to prevent unauthorized access to your data.



To secure Time Machine preferences:

1. Open Time Machine preferences.
2. Slide the switch to "ON."

 A screen similar to the following appears:



3. Select the disk where backups will be stored, and click "Use for backup."

From the Command Line:

```
# Securing Time Machine Preferences
# --------------------------------
# Enable Time Machine
defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1
```

Securing Universal Access Preferences

Universal Access preferences are disabled by default. If you don't use an assistive device there are no security-related issues. However, if you use an assistive device, follow these guidelines:

- See the device manual for prevention of possible security risks.
- Enabling VoiceOver configures the computer to read the contents under the cursor out loud, which might disclose confidential data.
- These devices allow access to the computer that could reveal information in a compromising manner.

Securing Data and Using Encryption

7

Use this chapter to learn how to set POSIX, ACL, and global file permissions, to encrypt home folders and portable files, and to securely erase data.

Your data is the most valuable part of your computer. By using encryption you can protect data in the case of an attack or theft of your mobile computer.

By setting global permissions, encrypting home folders, and encrypting portable data you can be sure your data is secure. In addition, by using the secure erase feature of Leopard, deleted data is completely erased from the computer.

Permissions

You protect files and folders by setting permissions that restrict or allow users to access them. Leopard supports two methods of setting file and folder permissions:

- Portable Operating System Interface (POSIX) permissions—standard for UNIX operating systems.
- Access Control Lists (ACLs) permissions—used by Mac OS X and compatible with Microsoft Windows Server 2003 and Microsoft Windows XP.

ACL uses POSIX when verifying file and folder permissions. The process ACL uses to determine if an action is allowed or denied includes specific rules called access control entries (ACEs). If no ACEs apply, standard POSIX permissions determine access.

Setting POSIX Permissions

Leopard bases file permissions on POSIX standard permissions such as file ownership and access. Each share point, file, and folder has read, write, and execute permission defined for three categories of users: owner, group, and everyone. You can assign four types of standard POSIX access permissions to a share point, folder, or file: Read & Write, Read Only, Write Only, and None.

Viewing POSIX Permissions

You can assign standard POSIX access permissions to these categories of users:

- Owner—This is a user who creates an item (file or folder) on the server is its owner and has Read & Write permissions for that folder. By default the owner of an item and the server administrator can change the item's access privileges (allow a group or everyone to use the item). The administrator can also transfer ownership of the shared item to another user.
- Group—You can put users who need the same access to files and folders into group accounts. Assign access permissions to a shared item to one group only. For more information about creating groups, see the *User Management* guide.
- Everyone—This is any user who can log in to the file server (registered users and guests).

Before setting or changing POSIX permissions, view the current permission settings.

To view folder or file permissions:

1. Open Terminal.
2. Run the `ls` command:

```
$ ls -l
```

Output similar to the following appears:

```
computer:~/Documents ajohnson$ ls -l
total 500
drwxr-xr-x 2 ajohnson staff    68 Apr 28 2006 NewFolder
-rw-r--r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

Note: The "~" refers to your home folder, which in this case is /Users/ajohnson. ~/Documents/ is the current working folder.

You can also use the Finder to view POSIX permissions. In the Finder, Control-click a file and choose Get Info. Open the Ownership & Permissions disclosure triangle to view POSIX permissions.

Interpreting POSIX Permissions

To interpret POSIX permissions, read the first 10 bits of the long format output listed for a file or folder. For example:

```
drwxr-xr-x 2 ajohnson staff    68 Apr 28 2006 NewFolder
-rw-r--r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

In this example, `NewFolder` has the POSIX permissions `drwxr-xr-x` and has an owner and group of `ajohnson`. Permissions are as follows:

- The `d` of the POSIX permissions signifies that `newfolder` is a folder.
- The first three letters after the `d` (`rwx`) signify that the owner has read, write, and execute permission for that folder.
- The next three characters, `r-x`, signify that the group has read and execute permission.
- The last three characters, `r-x`, signify that all others have read and execute permission.

In this example, users who can access ajohnson's ~/Documents/ folder can open the NewFolder folder but can't modify or open the file.txt file. Read POSIX permissions are propagated through the folder hierarchy.

Although `NewFolder` has `drwxr-xr-x` privileges, only `ajohnson` can access the folder. This is because ajohnson's ~/Documents/ folder has `drwx------` POSIX permissions.

By default, most user folders have `drwx------` POSIX permissions. However, only the ~/, ~/Sites/, and ~/Public/ folders have `drwxr-xr-x` permissions. These permissions allow other people to view folder contents without authenticating. If you don't want other people to view the contents, change the permissions to `drwx------`.

In the ~/Public/ folder, the Drop Box folder has `drwx-wx-wx` POSIX permissions. This allows other users to add files into ajohnson's drop box but they can't view the files.

You might see a `t` for others' privileges on a folder used for collaboration. This `t` is sometimes known as the sticky bit. Enabling the sticky bit on a folder prevents people from overwriting, renaming, or otherwise modifying other people's files. This can be common if several people are granted `rwx` access.

The sticky bit being set can appear as `t` or `T`, depending on whether the execute bit is set for others:

- If the execute bit appears as `t`, the sticky bit is set and has searchable and executable permissions.
- If the execute bit appears as `T`, the sticky bit is set but does not have searchable or executable permissions.

For more information, see the `sticky` man page.

Modifying POSIX Permissions

After your determine current POSIX permission settings, you can modify them using the `chmod` command.

To modify POSIX permission:

1. In Terminal, enter the following to add write permission for the group to file.txt:

```
$ chmod g+w file.txt
```

2. View the permissions using the `ls` command.

```
$ ls -l
```

3. Validate that the permissions are correct.

```
computer:~/Documents ajohnson$ ls -l
total 12346
drwxr-xr-x 2 ajohnson staff    68 Apr 28 2006 NewFolder
-rw-rw-r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

For more information, see the `chmod` man page.

Setting File and Folder Flags

You can also protect files and folders by using flags. These flags, or permission extensions, override standard POSIX permissions. They can only be set or unset by the file's owner or an administrator using `sudo`. Use flags to prevent the system administrator (root) from modifying or deleting files or folders.

To enable and disable flags, use the `chflags` command.

Viewing Flags

Before setting or changing file or folder flags, view the current flag settings.

To display flags set on a folder:

```
$ ls -lo secret
-rw-r--r-- 1 ajohnson staff uchg 0 Mar  1 07:54 secret
```

This example displays the flag settings for a folder named secret.

Modifying Flags

After your determine current file or folder flag settings, modify them using the `chflags` command.

To lock or unlock a folder using flags:

```
$ sudo chflags uchg folderName
```

In this example, the folder named secret is locked.

To unlock the folder, change `uchg` to `nouchg`:

```
$ sudo chflags nouchg secret
```

WARNING: There is an `schg` option for the `chflags` command. It sets the system immutable flag. This setting can only be undone when the computer is in single-user mode. If this is done on a RAID, XSan, or other storage device that cannot be mounted in single user mode, the only way to undo the setting is to reformat the RAID or XSan device.

For more information, see the `chflags` man page.

Setting ACL Permissions

For greater flexibility in configuring and managing file permissions, Leopard Server implements ACLs. An ACL is an ordered list of rules called ACEs that control file permissions. Each ACE contains the following components:

- User—owner, group, and other
- Action—read, write, or execute
- Permission—allow or deny the action

The rules specify the permissions to be granted or denied to a group or user and controls how the permissions are propagated through a folder hierarchy.

ACLs in Leopard Server let you set file and folder access permissions for multiple users and groups, in addition to standard POSIX permissions. This makes it easy to set up collaborative environments for file sharing and uninterrupted workflows without compromising security.

Leopard Server has implemented file system ACLs that are fully compatible with Microsoft Windows Server 2003 and Windows XP.

To determine if an action is allowed or denied, ACEs are considered in order. The first ACE that applies to a user and action determines the permission and no further ACEs are evaluated. If no ACEs apply, standard POSIX permissions determine access.

Enabling ACL Permissions

By default, ACLs are enabled in Leopard Server. If they have somehow been turned off, you must enable the volume to support ACLs.

The following example uses the `fsaclctl` command to enable ACLs on a Leopard Server startup volume:

```
$ sudo /usr/sbin/fsaclctl -p / -e
```

For more information, enter `fsaclctl` in a Terminal window.

Modifying ACL Permissions

You can set ACL permissions for files. The `chmod` command enables an administrator to grant read, write, and execute privileges to specific users for a single file.

To set ACL permissions for a file:

1. Allow specific users to access specific files.

 For example, to allow Anne Johnson permission to read the file secret.txt, enter the following in Terminal:

   ```
   $ chmod +a “ajohnson allow read” secret.txt
   ```

2. Allow specific groups of users to access specific files.

 For example, to allow the engineers group permission to delete the file secret.txt, enter the following in Terminal:

   ```
   $ chmod +a “engineers allow delete” secret.txt
   ```

3. Deny access privileges to specific files.

 For example, to prevent Tom Clark from modifying the file secret.txt, enter the following in Terminal:

   ```
   $ chmod +a “tclark deny write” secret.txt
   ```

4. View and validate the ACL modifications with the `ls` command:

   ```
   $ ls -le secret.txt
   -rw------- 1 ajohnson admin 43008 Apr 14 2006 secret.txt
   0: ajohnson allow read
   1: tclark deny write
   2: engineers allow delete
   ```

 For more information, enter `man chmod` in a Terminal window.

Changing Global Umask for Stricter Default Permissions

Every file or folder has POSIX permissions associated with it. When you create a file or folder, the umask setting determines these POSIX permissions.

The umask value is subtracted from the maximum permissions value (777) to determine the default permission value of a newly created file or folder. For example, a umask of 022 results in a default permission of 755.

The default umask setting 022 (in octal) removes group and other write permissions. Group members and other users can read and run these files or folders. Changing the umask setting to 027 enables group members to read files and folders and prevents others from accessing the files and folders. If you want to be the only user to access your files and folders, set the umask setting to 077.

To change the globally defined umask setting, change the umask setting in /etc/launchd.conf.

You must be logged in as a user who can use `sudo` to perform these operations and you must use the decimal equivalent, not an octal number.

Note: Users and applications can override default umask settings at any time for their own files.

> ***WARNING:*** Many installations depend on the default umask setting. There can be unintended and possibly severe consequences to changing it. Instead, use inherited permissions, which are applied by setting permissions on a folder. All files contained in that folder will inherit the permissions of that folder.

To change the global umask file permission:

1. Sign in as a user who can use `sudo`.
2. Open Terminal.
3. Change the umask setting:

   ```
   $ sudo echo “umask 027” >> /etc/launchd.conf
   ```

 This example sets the global umask setting to 027.
4. Log out.

Changes to umask settings take effect at the next login.

Users can use the Finder’s Get Info window or the `chmod` command-line tool to change permissions for files and folders.

Restricting Setuid Programs

When applied to a program, the POSIX setuid (set user ID) permission means that when the program runs, it will run at the privilege level of the file's owner. The POSIX setgid (set group ID) permission is analogous. To see an example of a file with the setuid bit, run the ls command on the ping program as follows:

```
$ ls -l /sbin/ping
-r-sr-xr-x  1 root  wheel  68448 Nov 28  2007 /sbin/ping
```

The setuid bit is represented with an 's' in the field of permissions, in the position that contains the file owner's execute permission. The program runs with the privilege level of the file's owner. The owner of the file is root, so when ping is executed—no matter who actually executes it—it runs as root. For setgid programs, an 's' appears in the group execute permission and the file runs with the privileges of the group owner.

The setuid bit is necessary in order for many programs on the system to perform the specific, privileged tasks for which they are designed. The ping program, for example, is setuid because it needs to be able to engage in some network communication that is only possible with root privileges.

To find setuid programs on the system, use the following command:

```
$ sudo find / -perm -04000 -ls
```

To find setgid programs, use -02000 instead of -04000.

Mac OS X includes approximately 75 setuid programs. Many of these programs need the setuid bit for normal system operation. However, other programs may need the setuid bit only if certain functionality is needed, or only if administrators need to use the program. Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program. If a program is needed but has had its setuid bit stripped, an administrator can run the program using sudo, which runs the program as the root user. An administrator can also temporarily enable the setuid bit while the program is needed, and then disable it again afterward.

Stripping Setuid Bits

To strip the setuid or setgid bit from a program, use the following command:

```
$ sudo chmod -s programname
```

The following programs can have their setuid bit removed, unless needed for the purpose shown in the second column:

Application	Related Service
/System/Library/CoreServices/ RemoteManagement/ ARDAgent.app/Contents/ MacOS/ARDAgent	Apple Remote Desktop
/System/Library/Extensions/ webdav_fs.kext/Contents/ Resources/load_webdav	WebDAV Web Services
/System/Library/Filesystems/ AppleShare /afpLoad	Apple File Protocol
/System/Library/Filesystems/ AppleShare/check_afp.app/ Contents/MacOS/check_afp	Apple File Protocol Sharing
/System/Library/Frameworks/ ApplicationServices.framework/ Versions/A/Frameworks/ PrintCore.framework/Versions/A/ Resources/PrinterSharingTool	Printer Sharing
/System/Library/CoreServices/ Expansion Slot Utility.app/ Contents/ Resources/PCIELaneConfigTool	Expansion Slot Utility
/System/Library/ PrivateFrameworks/ DesktopServicesPriv.framework/ Versions/A/Resources/Locum	Performing Privileged File Operations using Finder
/System/Library/Printers/ Libraries/aehelper	Printer Configuration
/System/Library/Printers/ Libraries/csregprinter	Printer Configuration
/System/Library/ PrivateFrameworks/ DiskManagement.framework/ Versions/A/ Resources/DiskManagementTool	Disk Utility
/usr/libexec/dumpemacs	N/A
/usr/libexec/xgrid/IdleTool	XGrid
/usr/libexec/statsCollector	Network BigTop
/usr/sbin/vpnd	Hosting VPN Services

Application	Related Service
/sbin/mount_nfs	Mounting NFS Filesystems
/sbin/route	Network Configuration
/usr/bin/lppasswd	Printer Sharing
/usr/bin/ipcs	IPC Statistics
/bin/rcp	Remote Access (insecure)
/usr/bin/rlogin	Remote Access (insecure)
/usr/bin/rsh	Remote Access (insecure)
/usr/lib/sa/sadc	System Activity Reporting
/usr/sbin/pppd	PPP
/usr/sbin/scselect	Allowing non-administrators to change Network Location

Important: The "Repair Permissions" feature of Disk Utility re-enables the setuid bit on these programs. Software updates may also re-enable the setuid bit on these programs. In order to achieve some persistence for the permissions change, create a shell script to strip the bits and then implement a cron job (for the root account) to execute this script every half hour. This ensures that no more than half an hour passes from the time a system update is applied until the setuid bits are removed. For information about how to set up a cron job, consult *Command-Line Administration*, available at http://www.apple.com/server/macosx/resources/.

Using ACLs to Restrict Usage of Setuid Programs

The ACL feature of Mac OS X can also be used to restrict the execution of setuid programs. Restricting the execution of setuid programs to administrators prevents other users from executing those programs. It should also prevent attackers who are currently running with ordinary user privileges from executing the setuid program and trying to elevate their privileges. All users on the system are in the "staff" group, so the commands below allow members of the admin group to execute <program name>, but deny that right to members of the staff group:

```
$ sudo chmod +a "group:staff deny execute" <program name>
$ sudo chmod +a# 0 "group:admin allow execute" <program name>
```

To view the ACL:

```
$ ls -le <program name>
```

The output looks something like this:

```
-r-sr-xr-x+ 1 root wheel 12345 Nov 28 2007 <program name>
0: group:admin allow execute
1: group:staff deny execute
```

Because the ACL is evaluated in order from top to bottom, users in the admin group are permitted to execute the program. The following rule denies that right to all users.

Important: Although the "Repair Permissions" feature of Disk Utility does not strip ACLs from programs, software updates might strip these ACLs. In order to achieve some persistence for the ACLs, create a shell script to set the ACLs and then implement a cron job (for the root account) to execute this script. For information about how to set up a cron job, consult *Command-Line Administration*, available at http://www.apple.com/server/macosx/resources/.

A cron job should ensure that no longer than an understood time period should pass from the time a system update is applied and the ACL is reset. Because the ACL described above uses the +a# option to place rules in a non-canonical order, its reapplication results in additional rules. The following script can successfully apply – and reapply – the rules:

```
chmod –a “group:admin allow execute” <program name>
chmod +a “group:staff deny execute” <program name>
chmod +a# 0 “group:admin allow execute” <program name>
```

Securing User Home Folders

To secure user home folders, change the permissions of each user's home folder so the folder is not world-readable or world-searchable.

When FileVault is not enabled, the permissions on the home folder of a new user account allow other users to browse the folder's contents. However, users might inadvertently save sensitive files to their home folder, instead of into the more-protected ~/Documents, ~/Library, or ~/Desktop folders.

The ~/Sites, ~/Public, and ~/Public/Drop Box folders in each home folder may require world-readable or world-writeable permissions if File Sharing or Web Sharing is enabled. If these services are not in use, the permissions on these folders can be safely changed to prevent other users from browsing or writing to their contents.

To change home folder permissions:

Enter the following command:

```
$ sudo chmod 700 /Users/username
```

Replace *username* with the name of the account.

Run this command immediately after someone creates an account.

In Leopard Server all users are a member of the "staff" group, not of a group that has the same name as their user name.

Note: Changing permissions on a user's home directory from 750 to 700 will disable Apple file sharing (using the ~/Public directory) and Apple web sharing (using the ~/Sites directory).

As the owner of his or her home folder, the user can alter the folder's permission settings at any time, and can change these settings back.

Encrypting Home Folders

Leopard includes FileVault, which can encrypt your home folder and its files. Use FileVault on portable computers and other computers whose physical security you can't guarantee. Enable FileVault encryption for your computer and its user accounts.

FileVault moves all content of your home folder into a bundle disk image that supports AES-128 encryption. Leopard supports Tiger sparse disk image created using AES-128 encryption. The sparse format allows the image to maintain a size proportional to its contents, which can save disk space.

If you remove files from a FileVault-protected home folder it takes time to recover free space from the home folder. After the home folder is optimized, you can access files in FileVault-protected home folders without noticeable delays.

If you're working with confidential files that you plan to erase later, store those files in separate encrypted images that are not located in your home folder. You can then erase those images without needing to recover free space. For more information, see "Encrypting Portable Files" on page 166.

If you've insecurely deleted files before using FileVault, these files are recoverable after activating it. To prevent this, when you initially enable FileVault, securely erase free space. For information, see "Using Disk Utility to Securely Erase Free Space" on page 171.

Because FileVault is an encryption of a user's local home folder, FileVault does not encrypt or protect files transferred over the network or saved to removable media, so you'll need to encrypt specific files or folders. FileVault can only be enabled for local or mobile accounts and cannot be enabled for network home folders.

If you want to protect file or folders on portable media or a network volume, you must create an encrypted disk image on the portable media or network volume. You can then mount these encrypted disk images, which protect data transmitted over the network using AES-128 encryption. When using this method, you must only mount the encrypted disk image from one computer at a time to prevent irreparable corruption to the image content.

For information about encrypting specific files or folders for transfer from your network home folder, see "Encrypting Portable Files" on page 166.

When you set up FileVault, you create a master password. If you forget your login password, you can use your master password to recover encrypted data. If you forget your login password and your master password, you cannot recover your data. Because of this, consider sealing your master password in an envelope and storing it in a secure location.

You can use Password Assistant to help create a complex master password that cannot be easily compromised. For information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.

Enabling FileVault copies data from your home folder into an encrypted home folder. After copying, FileVault erases the unencrypted data.

By default FileVault insecurely erases the unencrypted data, but if you enable secure erase, your unencrypted data is securely erased.

Overview of FileVault

Leopard Server extends the unlocking of FileVault to Smart Cards, which provides the most secure practice for protecting FileVault accounts.

Accounts protected by FileVault support authentication using a passphrase or a Smart Card. With Smart Card authentication, the AES-256 symmetric Data Key (DK) used to encrypt the user's data is unwrapped using a private (encryption) key on the Smart Card. The data written to or read from disk is encrypted and decrypted on the fly during access.

FileVault encrypts the Data Key (DK) using the User Key (UK1), which can be generated from your passphrase or from the public key on your Smart Card. FileVault separately encrypts the Data Key using the FileVault Master Key (MK).

The architectural design of FileVault makes it possible for the MK and UK1 to encrypt and decrypt files. Providing strong encryption protects user data at rest while ensuring access management by IT staff.

The easiest method for centralized management of FileVault on a client computer is to use Leopard Server and WorkGroup Manager to enforce the use of FileVault and the proper identity.

Managing FileVault

You can set a FileVault master keychain to decrypt an account that uses FileVault to encrypt data. Then if a user forgets their FileVault account password (which he or she uses to decrypt encrypted data) you can use the FileVault master keychain to decrypt the data.

To create the FileVault master keychain:

1. Open System Preferences > Security.
2. Click Master Password and set a master password.

 Select a strong password and consider splitting the password into at least two components (first half and second half). You can use Password Assistant to ensure that the quality of the password is strong.

 To avoid having one person know the full password, have separate security administrators keep each password component. This prevents a single person from unlocking (decrypting) a FileVault account. For more information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.

 Setting a master password creates a keychain called FileVaultMaster.keychain in /Library/Keychains/. The FileVault master keychain contains a FileVault recovery key (self-signed root certificate) and a FileVault master password key (private key).
3. Delete the certificate named FileVaultMaster.cer in the same location as the FileVaultMaster.keychain.

 FileVaultMaster.cer is only used for importing the certificate into the keychain. This is only a certificate and does not contain the private key, so there is no security concern about someone with gaining access to this certificate.
4. Make a copy of FileVaultMaster.keychain and put it in a secure place.
5. Delete the private key from FileVaultMaster.keychain created on the computer to modify the keychain.

 Deleting the key ensures that even if someone unlocks the FileVault master keychain they cannot decrypt the contents of a FileVault account because there is no FileVault master password private key available for the decryption.

Managing the FileVault Master Keychain

The modified FileVault master keychain can now be distributed to network computers. This can be done by transferring FileVaultMaster.keychain to the computers by using Apple Remote Desktop, by using a distributed installer executed on each computer, by using various scripting techniques, or by including it in the original disk image if your organization restores systems with a default image.

The master keychain provides network management of any FileVault account created on any computer with the modified FileVaultMaster.keychain located in the /Library/Keychains/ folder. These computers indicate that the master password is set in Security preferences.

When an account is created and the modified FileVault master keychain is present, the public key from the FileVault recovery key is used to encrypt the dynamically generated AES 128-bit (default) or AES 256-bit symmetric key that is used for the encryption and decryption of the encrypted disk image (FileVault container).

To decrypt access to the encrypted disk image, the FileVault master password private key is required to decrypt the original dynamically generated AES 128-bit or 256-bit symmetric key. The user's original password continues to work as normal, but the assumption here is that the master password service is being used because the user has forgotten the password or the organization must perform data recovery from a user's computer.

To recover a network managed FileVault system account:

1. Retrieve the copy of FileVaultMaster.keychain that was stored before the private key was deleting during modification.
2. Bring together all security administrators involved in generating the master password.

 More than one individual is needed if the master password was split into password components.

 Note: The administrator must have root access to restore the FileVaultMaster.keychain file.
3. Restore the original keychain to the /Library/Keychains/ folder of the target computer, replacing the installed keychain.
4. Verify that the restored FileVaultMaster.keychain file has the correct ownership and permissions set, similar to the following example.

   ```
   -rw-r--r-- 1 root admin 24880 Mar 2 18:18 FileVaultMaster.keychain
   ```
5. Verify that "Password Hints" is enabled by logging in to the FileVault account you are attempting to recover and incorrectly enter the account password three times.

 If "Password Hints" is enabled, you are granted an additional try after the hint appeals.
6. When prompted for the master password, have the security administrators combine their password components to unlock access to the account.
7. When the account is unlocked, provide a new password for the account.

 The password is used to encrypt the original symmetric key used to encrypt and decrypt the disk image.

 Note: This process does not reencrypt the FileVault container. It reencrypts the original symmetric key with a key derived from the new user account password you entered.

You are now logged in to the account and given access to the user's home folder.

8 Delete the private key from FileVaultMaster.keychain again, or replace the keychain file with the original copy of FileVaultMaster.keychain that was stored before the private key was deleted.

This process does not change the password used to protect the user's original login keychain, because that password is not known or stored anywhere. Instead, this process creates a login keychain with the password entered as the user's new account password.

Encrypting Portable Files

To protect files you want to transfer over a network or save to removable media, encrypt a disk image or encrypt the files and folders. FileVault doesn't protect files transmitted over the network or saved to removable media.

Using a server-based encrypted disk image provides the added benefit of encrypting network traffic between the computer and the server hosting the mounted encrypted disk image.

Creating an Encrypted Disk Image

To encrypt and securely store data, you can create a read/write image or a sparse image:

- A read/write image consumes the space that was defined when the image was created. For example, if the maximum size of a read/write image is set to 10 GB, the image consumes 10 GB of space even if it contains only 2 GB of data.
- A sparse image consumes only the amount of space the data needs. For example, if the maximum size of a sparse image is 10 GB and the data is only 2 GB, the image consumes only 2 GB of space.

If an unauthorized administrator might access your computer, creating an encrypted blank disk image is preferred to creating an encrypted disk image from existing data.

Creating an encrypted image from existing data copies the data from an unprotected area to the encrypted image. If the data is sensitive, create the image before creating the documents. This creates the working copies, backups, or caches of files in encrypted storage from the start.

Note: To prevent errors when a file system inside a sparse image has more free space than the volume holding the sparse image, HFS volumes inside sparse images will report an amount of free space slightly less than the amount of free space on the volume that the image resides on.

To create an encrypted disk image:

1. Open Disk Utility.
2. Choose File > New > Blank Disk Image.
3. Enter a name for the image, and choose where to store it.
4. Choose the size of the image by clicking the Size pop-up menu.

 Make sure the size of the image is large enough for your needs. You cannot increase the size of an image after creating it.
5. Choose an encryption method by clicking the Encryption pop-up menu.

 AES-128 or AES-256 is a strong encryption format.
6. Choose a format by clicking the Format pop-up menu.

 Although there is some overhead, the sparse format allows the image to maintain a size proportional to its contents (up to its maximum size), which can save disk space.
7. Click Create.
8. Enter a password, and verify it.

 You can access Password Assistant from this window. For more information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.
9. Deselect "Remember password (add to Keychain)," and click OK.

Creating an Encrypted Disk Image from Existing Data

If you must maintain data confidentiality when transferring files from your computer but you don't need to encrypt files on your computer, create a disk image from existing data.

Such situations include unavoidable plain-text file transfers across a network, such as mail attachments or FTP, or copying to removable media, such as a CD or floppy disk.

If you plan to add files to this image instead of creating an image from existing data, create an encrypted disk image and add your existing data to it. For information, see "Creating an Encrypted Disk Image" on page 166.

To create an encrypted disk image from existing data:

1. Open Disk Utility.
2. Choose File > New > Disk Image from Folder.
3. Select a folder, and click Image.
4. Choose File > New > Blank Disk Image.
5. Enter a name for the image and choose where to store it.
6. Choose a format by clicking the Format pop-up menu.

The compressed disk image format can help you save hard disk space by reducing your disk image size.

7 Choose an encryption method by clicking the Encryption pop-up menu.

AES-128 or AES-256 provide strong encryption.

8 Click Save.

9 Enter a password and verify it.

You can easily access Password Assistant from this window. For more information, see "Using Password Assistant to Generate or Analyze Passwords" on page 103.

10 Deselect "Remember password (add to Keychain)" and click OK.

You can also use the `hdiutil` command to create and format encrypted disk images. For more information about this command, see its man page.

Creating Encrypted PDFs

You can quickly create password-protected, read-only PDF documents of confidential or personal data. To open these files you must know the password for them.

Some applications do not support printing to PDF. In this case, create an encrypted disc image. For information, see "Creating an Encrypted Disk Image from Existing Data" on page 167.

To create an encrypted, read-only document:

1 Open the document.

2 Choose File > Print.

Some applications don't allow you to print from the File menu. These applications might allow you to print from other menus.

3 Click PDF and choose Save as PDF.

4 Click Security Options and select one or more of the following options:

- Require password to open document
- Require password to copy text images and other content
- Require password to print document

When you require a password for the PDF, it becomes encrypted.

5 Enter a password, verify it, and click OK.

6 Enter a name for the document, choose a location, and click Save.

7 Test your document by opening it.

You must enter the password before you can view the contents of your document.

Securely Erasing Data

When you erase a file, you're removing information that the file system uses to find the file. The file's location on the disk is marked as free space. If other files have not written over the free space, it is possible to retrieve the file and its contents.

Leopard provides the following ways to securely erase files.

- Zero-out erase
- 7-pass erase
- 35-pass erase

A zero-out erase sets all data bits on the disk to 0, while a 7-pass erase and a 35-pass erase use algorithms to overwrite the disk. A 7-pass erase follows the Department of Defense standard for the sanitization of magnetic media. A 35-pass erase uses the extremely advanced Gutmann algorithm to help eliminate the possibility of data recovery.

The zero-out erase is the quickest. The 35-pass erase is the most secure, but it is also 35 times slower than the zero-out erase.

Each time you use a 7-pass or 35-pass secure erase, the following seven-step algorithm is used to prevent the data from being recovered:

- Overwrite file with a single character
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters

Configuring Finder to Always Securely Erase

In Leopard Server you can configure Finder to always securely erase items placed in the Trash. This prevents data you place in the Trash from being restored. Using secure erase take longer than emptying the Trash.

To configure Finder to always perform a secure erase:

1. In Finder, choose Finder > Preferences.
2. Click Advanced.
3. Select the "Empty Trash securely" checkbox.

Using Disk Utility to Securely Erase a Disk or Partition

You can use Disk Utility to securely erase a partition, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

Note: If you have a partition with Leopard installed and you want to securely erase an unmounted partition, you don't need to use your installation discs. In the Finder, open Disk Utility (located in /Applications/Utilities/).

> *WARNING:* Securely erasing a partition is irreversible. Before erasing the partition, back up critical files you want to keep.

To securely erase a partition using Disk Utility:

1. Insert the first of the Leopard installation discs in the optical drive.
2. Restart the computer while holding down the C key.

 The computer starts up from the disc in the optical drive.
3. Proceed past the language selection step.
4. Choose Utilities > Disk Utility.
5. Select the partition you want to securely erase.

 Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.
6. Click Erase, choose "Mac OS Extended Journaled," and then click Security Options.

 Mac OS Extended disk formatting provides enhanced multiplatform interoperability.
7. Choose an erase option and click OK.
8. Click Erase.

 Securely erasing a partition can take time, depending on the size of the partition and the method you choose.

Using Command-Line Tools to Securely Erase Files

You can use the `srm` command in Terminal to securely erase files or folders. By using `srm`, you can remove each file or folder by overwriting, renaming, and truncating the file or folder before erasing it. This prevents other people from undeleting or recovering information about the file or folder.

For example, `srm` supports simple methods, like overwriting data with a single pass of zeros, to more complex ones, like using a 7-pass or 35-pass erase.

The `srm` command cannot remove a write-protected file owned by another user, regardless of the permissions of the directory containing the file.

> ***WARNING:*** Erasing files with `srm` is irreversible. Before securely erasing files, back up critical files you want to keep.

To securely erase a folder named secret:

```
$ srm -r -s secret
```

The `-r` option removes the content of the directory, and the `-s` option (simple) overwrites with a single random pass.

For a more secure erase, use the `-m` (medium) option to perform a 7-pass erase of the file. The `-s` option overrides the `-m` option, if both are present. If neither is specified, the 35-pass is used.

For more information, see the `srm` man page.

Using Secure Empty Trash

Secure Empty Trash uses a 7-pass erase to securely erase files stored in the Trash. Depending on the size of the files being erased, securely emptying the Trash can take time to complete.

> ***WARNING:*** Using Secure Empty Trash is irreversible. Before securely erasing files, back up critical files you want to keep.

To use Secure Empty Trash:

1. Open the Finder.
2. Choose Finder > Secure Empty Trash.
3. Click OK.

Using Disk Utility to Securely Erase Free Space

You can use Disk Utility to securely erase free space on partitions, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

To securely erase free space using Disk Utility:

1. Open Disk Utility (located in /Applications/Utilities/).
2. Select the partition to securely erase free space from.

 Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.
3. Click Erase, and then click Erase Free Space.
4. Choose an erase option and click Erase Free Space.

Securely erasing free space can take time, depending on the amount of free space being erased and the method you choose.

5 Choose Disk Utility > Quit Disk Utility.

Using Command-Line Tools to Securely Erase Free Space

You can securely erase free space from the command line by using the `diskutil` command. However, ownership of the affected disk is required. This tool allows you to securely erase using one of the three levels of secure erase:

- 1—Zero-out secure erase (also known as single-pass)
- 2—7-pass secure erase
- 3—35-pass secure erase

To erase free space using a 7-pass secure erase (indicated by the number 2):

```
$ diskutil secureErase freespace 2 /dev/disk0s3
```

For more information, see the `diskutil` man page.

From the Command Line:

```
# ------------------------------------------------------------------
# Using Disk Utility to Securely Erase Free Space
# ------------------------------------------------------------------
# Overwrite a device with zeroes.
diskutil zeroDisk /dev/device

# Secure erase (7-pass) free space on a volume.
diskutil secureErase freespace 2 /dev/device

# Secure erase (7-pass) a volume.
diskutil secureErase 2 /dev/device
```

Securing System Swap and Hibernation Storage

8

Use this chapter to protect data in swap files from being readable.

The data that an application writes to random-access memory (RAM) might contain sensitive information, such as user names and passwords. Mac OS X writes the contents of RAM to your local hard disk to free memory for other applications. The RAM contents stored on the hard disk are kept in a file called a swap file.

While the data is on the hard disk, it can be easily viewed or accessed if the computer is later compromised. You can protect this data by securing the system swap file in case of an attack or theft of your computer.

System Swap File Overview

When your computer is turned off, any information stored in RAM is lost, but information stored by virtual memory in a swap file may remain on your hard drive in unencrypted form. The Mac OS X virtual memory system creates this swap file in order to reduce problems caused by limited memory.

The virtual memory system can swap data between your hard disk and RAM. It's possible that sensitive information in your computer's RAM will be written to your hard disk in the swap file while you are working, and remain there until overwritten. This data can be compromised if your computer is accessed by an unauthorized user, because the data is stored on the hard disk unencrypted.

When your computer goes into hibernation, it writes the content of RAM to the /var/vm/sleepimage file. The sleepimage file contains the contents of RAM unencrypted, similar to a swap file.

You can prevent your sensitive RAM information from being left unencrypted on your hard disk by enabling secure virtual memory to encrypt the swap file and the /var/vm/sleepimage file (where your hibernation files are stored).

Note: Using FileVault in combination with the "Secure Virtual Memory" feature provides protection from attacks on your sensitive data when it is stored on the hard drive.

Encrypting System Swap

You can prevent your sensitive information from remaining on your hard disk and eliminate the security risk by using secure virtual memory. Secure virtual memory encrypts the data being written to disk.

To turn on secure virtual memory:

1. Open System Preferences.
2. Click Security, then click General.
3. Select "Use secure virtual memory."
4. Reboot.

From the Command Line:

```
# Securing System Swap and Hibernation Storage
# ----------------------------
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
     UseEncryptedSwap -bool YES
```

Avoiding Simultaneous Local Account Access

9

Use this chapter to limit local account access so you can more easily monitor activity on your computer.

Monitoring user accounts and activities is important to securing your computer. This enables you to determine if an account is compromised or if a user is performing malicious tasks.

Fast User Switching

Although the use of Fast User Switching is convenient when you have multiple users on a single computer, avoid enabling it.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is using the computer.

Also, any external volumes attached to the computer are mounted when another user logs in, granting all users access to the volume and ignoring access permissions.

Shared User Accounts

Avoid creating accounts that are shared by several users. Individual accounts maintain accountability. Each user should have his or her own standard or managed account.

System logs can track activities for each user account, but if several users share the same account, it becomes difficult to track which user performed an activity. Similarly, if several administrators share a single administrator account, it becomes harder to track which administrator performed a specific action.

If someone compromises a shared account it is less likely to be noticed. Users might mistake malicious actions performed by an intruder for legitimate actions by a user sharing the account.

Ensuring Data Integrity with Backups

10

Use this chapter to learn about secure ways of backing up your data and preventing unauthorized access to your backups.

Most organizations perform backups to protect their data from being lost. However, many organizations don't consider that their backups can be compromised if the backups are not securely stored on media.

The Time Machine Architecture

Time Machine is based on the Mac OS X HFS+ file system. It tracks file changes and detects file system permissions and user access privileges.

When Time Machine performs the initial backup, it copies the contents of your computer to your backup drive. Every subsequent backup is an incremental backup, which copies only the files that have changed since the previous backup.

Deleting Permanently from Time Machine Backups

You can permanently delete files or folders from your computer and all Time Machine backups using Time Machine. This keeps sensitive data that you no longer need from being recovered.

To permanently delete files or folders from Time Machine backups:

1. Delete the file or folder from your computer.
2. Open Time Machine.
3. Select the file for folder you want to permanently delete from Time Machine.
4. Click the Action pop-up menu and select "Delete All Backups of "*File or Folder name*."
5. When the warning message appears, click OK to permanently delete the file or folder.

 All backup copies of your file or folder are permanently deleted from your computer.

Storing Backups Inside Secure Storage

You can also perform backups of specific files or folders that contain sensitive data by placing your data in an encrypted disk image. This image can then be placed on any server that is backed up regularly and still maintains the integrity of your data because it is protected by encryption.

For example, Mac computer users in a Windows Server environment can use this method of backing up to ensure that sensitive data is secure and regularly backed up.

To securely encrypt and back up your data:

1. Create a disk image.

 For more information about creating a disk image, see "Encrypting Portable Files" on page 166.
2. Mount the disk image.
3. Copy the files you want to back up to the disk image.
4. Unmount the image and copy it to your backup media.

 If you're in a Windows Server environment, copy your image to a folder that is backed up by the Windows server. Your data will be both encrypted and backed up.

Restoring Backups from Secure Storage

If you accidentally delete or lose the file, you can restore it from your encrypted backup media.

To restore from an encrypted backup:

1. Access the media that contains your disk image backup.
2. Mount the disk image and, if prompted, enter your password for the image file.

 If the image is on a network, you don't need to copy it locally. It will securely mount across the network because the data is encrypted.
3. Copy the backup of the file you lost locally to your computer.
4. Unmount the disk image.

Securing Accounts and Share Points

11

Use this chapter to learn how to use Server Admin and Workgroup Manager to set up and manage home folders, accounts, and settings for clients.

Leopard Server includes Server Admin and Workgroup Manager.

You can use Server Admin to create and manage share points.

You can use Workgroup Manager, a user management tool, to manage user, group, computer, and computer group accounts. You can define core account settings like name, password, home folder location, and group membership. You can also manage preferences, allowing you to customize the user's experience, granting or restricting access to his or her computer's settings and to network resources.

Workgroup Manager works closely with a directory domain. Directory domains are like databases, only they are specifically geared towards storing account information and handling authentication. For more information about Open Directory, see Chapter 24, "Securing Directory Services."

For information about using Workgroup Manager, see the *User Management* guide.

Open Directory and Active Directory

Leopard Server supports Open Directory and Active Directory domains for client authentication.

Open Directory uses OpenLDAP, the open source implementation of Lightweight Directory Access Protocol (LDAP), to provide directory services. It's compatible with other standards-based LDAP servers, and can be integrated with proprietary services such as Microsoft's Active Directory and Novell's eDirectory. For more information about how to configure these options, see "Configuring Open Directory Policies" on page 338.

The Active Directory plug-in supports packet signing and packet encryption and is set to "allow," which means it negotiates the connection by default and can be changed to "require" if needed. Also, if you connect to an Active Directory server with Highly Secure (HISEC) templates enabled, you can use third-party tools to further secure your Active Directory connection.

Users can mutually authenticate with both Open Directory and Active Directory. Both use Kerberos to authenticate. Kerberos is a ticket-based system that enables mutual authentication. The server must identify itself by providing a ticket to a users' computer. This prevents your computer from connecting to rogue servers. Users must enable trusted binding to mutually authenticate with Open Directory or Active Directory.

For more information about Open Directory and Active Directory, see the *Open Directory Administration* guide.

Configuring Share Points

A share point is a hard disk (or hard disk partition), disc media, or folder that contains files you want users to share. You can use share points to host home folders.

You can use Server Admin to set up share points and then use the share points to host local home folders. Or you can mount the share point so it hosts network home folders.

Using network home folders stored on a share point is inherently less secure than using local home folders. An intruder can access your network home folder through an insecure network connection.

It is recommended that you make sure that all share points on local system drives are configured to grant access to only specific users or groups, and are not open to everyone. Removing open share points prevents unwanted access to your computer and prevents your computer from being used to maliciously access additional computers on the network. It is also recommended not to share files unnecessarily.

Disabling Share Points

Disable unused share points and sharing protocols. Enabled share points and sharing protocols can provide an avenue of attack for intruders.

If you disable all share points using a specific sharing protocol, you should also disable that protocol.

To disable a share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Share Point below the list.

5 Click Protocol Options.

6 Disable the following sharing options:

Click AFP and deselect "Share this item using AFP."

Click SMB and deselect "Share this item using SMB."

Click FTP and deselect "Share this item using FTP."

Click NFS and deselect "Export this item and its contents to".

7 Click OK.

8 Click Save.

Restricting Access to a Share Point

Before enabling a share point, restrict the access permissions for the folder that will act as the share point and only allow users who must use the share point to access it.

You can then use Server Admin's File Sharing pane to set POSIX and ACL permissions to restrict share points to only being accessible by specific users. You can use a combination of the two permission types to customize accessibility for your users.

You can also use Workgroup Manager's effective permissions inspector to determine the permissions a user is granted.

> ***WARNING:*** Carefully set access permissions. Incorrectly set access permissions can prevent legitimate users from accessing folders and files, or they can allow malicious users to access folders and files.

To restrict access to a share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point from the list.

4 Click Permissions below the list.

5 To set the owner or group of the shared item, enter names or drag names from the Users and Groups drawer to the owner or group records in the permissions table.

The owner and group records are listed under the POSIX heading. The owner record has the single user icon. The group record has the group icon.

To open the drawer, click the Add (+) button. If you don't see a recently created user or group, click the Refresh button (below the Servers list).

Owner and group names can also be edited by double-clicking a permissions record and dragging into or typing in the User/Group field in the window that appears.

Note: To change the autorefresh interval, choose Server Admin > Preferences and change the value of the "Auto-refresh status every" field.

Make sure you understand the implications of changing a folder's owner and group. For more information, see "Setting POSIX Permissions" on page 151.

6 To change the permissions for Owner, Group, and Others, use the Permission pop-up menu in the related row of the permissions table.

Others is any user that logs in to the file server who is not the owner and does not belong to the group.

If you're configuring a home folder's permissions, give the owner Read & Write privileges, but reduce group and everyone privileges to None.

The default for home folders is that the staff group and everyone have read privileges. All accounts are also members of the staff group. These two privileges allow everyone to view the contents of the home folder. If you want someone other than the owner to view the contents of the home folder, replace staff with that account.

7 Click Save.

The new share point is shared using AFP, SMB, and FTP, but not NFS.

To set ACL permissions on a share point or a folder:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point from the list.

4 Click Permissions below the list.

5 Open the Users and Groups drawer by clicking the Add (+) button.

6 Drag groups and users from the drawer into the ACL Permissions list to create ACEs.

By default, each new ACE gives the user or group full read and inheritance permissions.

The first entry in the list takes precedence over the second, which takes precedence over the third, and so on. For example, if the first entry denies a user the right to edit a file, other ACEs that allow the same user editing permissions are ignored. In addition, the ACEs in the ACL take precedence over standard permissions.

7 In the Access Control List, select the ACE.

8 Click the Edit (/) button.

9 From the Permission Type pop-up menu, choose "Allow" or "Deny."

10 In the Permissions list, select permissions.

If you chose Custom from the Permission pop-up menu, click the disclosure triangles to display specific attributes. Choose Allow or Deny from the Permission Type pop-up menu. Select specific permissions and click OK.

You can further grant or deny specific permissions that you cannot specify through POSIX permissions. For example, you can allow a user to list folder contents but disallow that user from reading file attributes.

11 Click Save.

AFP Share Points

If you supply network home folders, use AFP because it provides authentication-level access security. A user must log in with a valid user name and password to access files.

You can also enable AFP using an SSH-secured tunnel for file sharing. This tunnel prevents intruders from intercepting your communication with an AFP share point. You cannot enable SSH-secured tunnels for AFP share points that host home folders.

For more information, see "Configuring AFP File Sharing Service" on page 278.

SMB Share Points

You should not use SMB unless you're hosting a share point specifically for Windows users. You can set up a share point for SMB access only, so that Windows users have a network location for files that can't be used on other platforms

Like AFP, SMB also requires authenticating with a valid user name and password to access files. However, there are well-known risks associated with SMB. For example, SMB uses NTLMv1 and NTLMv2 encryption, both of which are weak password hashing schemes.

For more information, see "Configuring SMB File Sharing Service" on page 283.

FTP Share Points

You cannot use FTP share points to host home folders and you should only enable FTP share points if you require anonymous access.

Files are transferred from FTP share points unencrypted over the network. Transferring files over FTP does not guarantee confidentiality or file integrity.

If you need to use FTP for file transfers, consider using the SSH service instead. The `sftp` command, part of the SSH suite of tools, will provide an FTP-like experience to an end user while providing a more secure setting. For more information, see the `sftp` man page.

For more information about setting up FTP share points, see "Configuring FTP File Sharing Service" on page 280.

NFS Share Points

NFS file access is not based on user authentication (entering a user name and password). It is based on the user ID and the client IP address. As such, NFS share points without the use of Kerberos don't have the same level of security as AFP and SMB, which require user authentication to gain access to a share point's contents.

If you have NFS clients, consider setting up a share point to be used only by NFS users, or configure NFS with Kerberos. NFS doesn't support SACLs.

Use NFS only if you must provide home folders for a large number of users who use UNIX workstations. Use Server Admin to restrict access to an NFS share point, so that only required computers can access it.

To restrict access to an NFS share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Share Point below the list.
5. Click Protocol Options.
6. Click NFS.
7. If only a few computers need access to the share point, select "Export this item and its contents to" and choose Client List from the pop-up menu.

 To add clients, click Add (+) and enter the IP address of the client computer.

 Add only those client computers that require access to the share point.
8. If every computer in a subnet requires access to the share point, select "Export this item and its contents to" and choose Subnet from the pop-up menu.

 In the Subnet address field, enter the subnet address. In the Subnet mask field, enter the subnet mask.
9. From the Mapping pop-up menu, choose "All to nobody."

 A user with "nobody" privileges has "Others" POSIX permissions.
10. From the Minimum Security pop-up menu, set the level of authentication:

 Choose "Standard" if you don't want to set a level of authentication.

 Choose "Any" if you want NFS to accept any method authentication.

 Choose "Kerberos v5" if you want NFS to only accept Kerberos authentication.

 Choose "Kerberos v5 with data integrity" if you want NFS to accept Kerberos authentication and validate the data (checksum) during transmission.

 Choose "Kerberos v5 with data integrity and privacy" to have NFS accept Kerberos authentication, to validate using the checksum, and to encrypt data during transmission.
11. Select "Read-only."
12. Click Save.

Controlling Network Views

Leopard Server doesn't support managed network views.

To manage network views hosted on servers running Tiger Server, use the Workgroup Manager included with Tiger Server.

Securing Accounts

You can modify several account settings to improve security. Check with your organization to ensure that these settings do not conflict with network settings or organizational requirements.

In Workgroup Manager, you can use presets to save your settings as a template for future accounts. If you have settings that you apply to several accounts, you can use presets to expedite the creation of these accounts. Using presets also ensures that you use uniform account settings and helps you avoid configuration errors. For more information, see the *User Management* guide.

Configuring User Accounts

If you want to manage individual users or if you want those users to have unique identities on your network, create user accounts.

Before creating or modifying user accounts, you should have a firm understanding of what the account will be used for and what authentication method you want to use.

To configure user accounts:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to work with.

 To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Basic.
5. If you want to grant server administration privileges to the user, select "administer this server."

 Server administration privileges allows the user to use Server Admin and make changes to a server's search policy using Directory Utility.
6. Click Advanced, then deselect "Allow simultaneous login on managed computers."

 By disallowing simultaneous login, you reduce the chances of version conflicts when loading and saving files. This helps remind users that they should log off of computers when they are not using them.

7 Choose the most secure password type available in the User Password Type pop-up menu.

If you don't use smart cards, you can choose Open Directory or crypt password. Open Directory is more secure than crypt password. If your network uses Open Directory for authentication, authenticate with it. For more information about Open Directory and crypt passwords, see the *Open Directory Administration* guide.

Smart cards are also a secure form of authentication. Smart cards use two-factor authentication, which helps ensure that your accounts are not compromised.

8 If you chose the Open Directory password type, click Options and complete the following:

a In the dialog that appears, select "Disable login on specific date" and enter the date that the user no longer needs the account.

b Select "Disable login after inactive for # days," and replace # with the number of days when the user no longer needs the account.

c Select "Disable login after user makes # failed attempts," and replace # with 3.

d Select "Allow the user to change the password."

e Select "Password must contain at least # characters," and replace # with 8.

f Select "Password must be reset every # days," and replace # with 90.

g If you want to require the user to create a password during their next login, select "Password must be changed at next login."

h Replace these suggested values with values that meet the requirements of your organization.

i Click OK.

9 Click Groups.

10 Click the Add (+) button to open a drawer listing all available groups, then drag groups from the drawer into the Primary Group ID field or the Other Groups list.

A primary group is the group a user belongs to if the user does not belong to other groups. If a user selects a different workgroup at login, the user still retains access permissions from the primary group.

The ID of the primary group is used by the file system when the user accesses a file he or she doesn't own. The file system checks the file's group permissions, and if the primary group ID of the user matches the ID of the group associated with the file, the user inherits group access permissions.

Adding a user to a group allows the user to access the group's group folder. Carefully choose which groups to add users to. For more information, see "Configuring Group Accounts" on page 187.

11 Click Home.

12 Select a secure location for the user's home folder in the home list and then enter an appropriate value in the Disk Quota field.

By using a disk quota, you prevent malicious users from performing a denial of service attack where they fill the home volume.

13 Click Mail and select None.

If you must enable mail, select POP only or IMAP only, but not both. Using fewer protocols reduces the number of possible avenues of attack.

14 Click Info.

15 Do not enter information in the user information fields provided.

User information can be used by malicious attackers when they try to compromise the user's account.

16 Click Windows and then click Save.

Configuring Group Accounts

Create groups of individuals with similar access needs. For example, if you create a separate group for each office, you can specify that only members of a certain office can log in to specific computers. When you more specifically define groups, you have greater control over who can use what.

You can grant or deny POSIX or ACL permissions to groups. If you have nested groups, you can propagate ACL permissions to child groups.

Groups also have access to group folders, which provide an easy way for group members to share files with each other.

To configure group accounts:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to work with.

To select an account, click the globe icon, choose the directory domain where the account resides, click the Groups button, and then select the group.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 In the Members pane, click the Add (+) button to open a drawer that lists the users and groups defined in the directory domain you're working with.

Make sure the group account resides in a directory domain specified in the search policy of computers that the user logs in to.

5 Click Group Folder.

6 In the Address list select a secure location for the group folder.

7 In the Owner Name fields, enter the short name and long name of the user you want to assign as the owner of the group folder so the user can act as group folder administrator.

To choose an owner from a list of users in the current directory domain, click the browse (…) button. Click the globe icon in the drawer to choose a different directory domain.

The group folder owner is given read/write access to the group folder.

8 Click Save.

Configuring Computer Groups

A computer group comprises computers with the same preference settings. You can use Workgroup Manager to create and modify computer groups.

Every computer on your network should be a member of a computer group. If you don't assign a computer to a computer group, the computer uses the managed preferences for the Guest Computer account.

By grouping computers into computer groups, you simplify the task of securing computers on your network.

To configure computer groups:

1 In Workgroup Manager, click Accounts.

2 Select the computer group.

To select the computer group, click the globe icon, choose the directory domain that contains the computer group, click the Computer Groups button, and then select the computer group.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click Members, click the Add (+) button, and then drag computers or computer groups from the drawer to the list.

You can also click the browse (…) button, select a computer, and then click Add.

Continue adding computers and computer groups until the list is complete.

5 Click Save.

Managing Certificates

12

Use this chapter to learn how Leopard Server supports services that ensure encrypted data transfer through certificates.

Leopard Server uses a Public Key Infrastructure (PKI) system to generate and maintain certificates of identities. Server Admin makes it easy to manage Secure Sockets Layer (SSL) certificates that can be used by Web, Mail, Open Directory, and other services that support them. You can create a self-signed certificate and generate a Certificate Signing Request (CSR) to obtain an SSL certificate from an issuing authority and install the certificate.

For more information about how to use SSL certificates with individual services, see Chapter 13, "Setting General Protocols and Access to Services." Also, for more information about certificates using the command line, see the man page of the `security` command-line tool.

Understanding Public Key Infrastructure

Leopard Server supports services that use SSL to ensure encrypted data transfer. It uses a PKI system to generate and maintain certificates for use with SSL-enabled services.

PKI systems allow the two parties in a data transaction to be authenticated to each other, and to use encryption keys and other information in identity certificates to encrypt and decrypt messages traveling between them.

PKI enables multiple communicating parties to establish confidentiality, message integrity, and message source authentication without exchanging secret information in advance.

SSL technology relies on a PKI system for secure data transmission and user authentication. It creates an initial secure communication channel to negotiate a faster, secret key transmission. Leopard Server uses SSL to provide encrypted data transmission for Mail, Web, and Directory services.

The following sections contain more background information about PKI:

- "Public and Private Keys" on page 190
- "Certificates" on page 190
- "CAs" on page 191
- "Identities" on page 191

Public and Private Keys

Within a PKI, two digital keys are created: the public key and the private key. The private key isn't distributed to anyone and is often encrypted by a passphrase. The public key is distributed to other communicating parties.

Basic key capabilities can be summed up as:

Key type	Capabilities
Public	• Can encrypt messages that can only by decrypted by the holder of the corresponding Private key. • Can verify the signature on a message to ensure that it is coming from a Private key.
Private	• Can digitally sign a message or certificate, claiming authenticity. • Can decrypt messages that were encrypted with the Public key. • Can encrypt messages that can only be decrypted by the Private key itself.

Web, Mail, and Directory services use the public key with SSL to negotiate a shared key for the duration of the connection.

For example, a mail server will send its public key to a connecting client and initiate negotiation for a secure connection. The connecting client uses the public key to encrypt a response to the negotiation. The mail server, because it has the private key, can decrypt the response. The negotiation continues until mail server and client have a shared secret to encrypt traffic between the two computers.

Certificates

A certificate is a piece of cryptographic information that enables the safe transfer of information over the Internet. Certificates are used by web browsers, mail applications, and online chat applications.

Public keys are often contained in certificates issued by a certificate authority (CA). A user can digitally sign messages using a private key; then, the receiver can verify the signature using the public key in the CA-issued certificate.

A public key certificate (sometimes called an identity certificate) is a file in a specified format (Leopard Server uses the x.509 format) that contains:

- The public key half of a public-private key pair
- The key user's identity information, such as a person's name and contact information
- A validity period (how long the certificate can be trusted to be accurate)

- The URL of someone with the power to revoke the certificate (its *revocation center*)
- The digital signature of a CA, or the key user

CAs

A CA is an entity that signs and issues digital identity certificates claiming that a party is correctly identified. In this sense, a CA is a trusted third party used by other parties when performing transactions.

In x.509 systems such as Leopard, CAs are hierarchical, with CAs being certified by higher CAs, until you reach a root authority. A root authority is a CA that's trusted by the parties, so it doesn't need to be authenticated by another CA. The hierarchy of certificates is top-down, with the root authority's certificate at the top.

A CA can be a company that signs and issues a public key certificate. The certificate attests that the public key belongs to the owner recorded in the certificate.

In a sense, a CA is a digital notary public. You request a certificate by providing the CA with your identity information, contact information, and the public key. The CA then verifies your information so users can trust certificates issued for you by the CA.

Identities

Identities, in the context of the Leopard Server Certificate Manager, include signed certificates for both keys of a PKI key pair. The identities are used by the system keychain and are available for use by various services that support SSL.

Self-Signed Certificates

Self-signed certificates are certificates that are digitally signed by the private key corresponding to the public key included in the certificate. This is done in place of a CA signing the certificate. By self-signing a certificate, you're attesting that you are who you say you are. No trusted third party is involved.

Obtaining Certificates

Before you can use SSL in Leopard Server's services, you must create or import certificates. You can create self-signed certificates, generate a Certificate Signing Request (CSR) to send to a CA, or import created certificates.

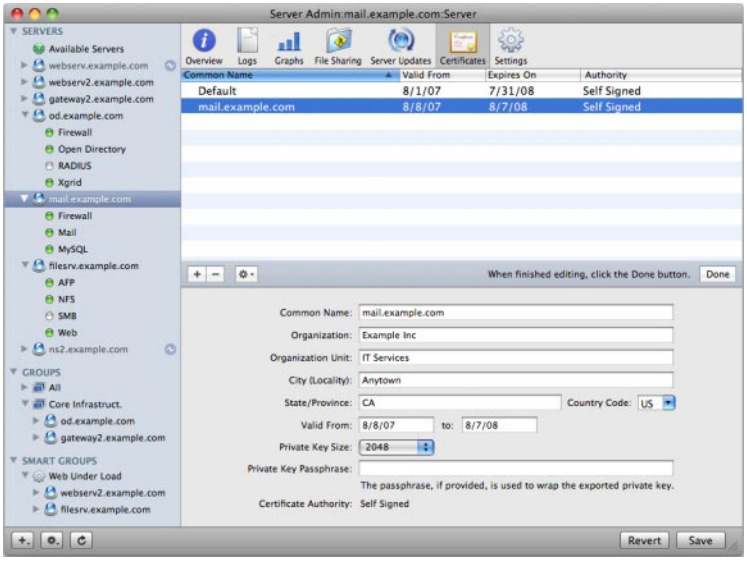
Select a CA to sign your certificate request. If you don't have a CA to sign your request, consider becoming your own CA, and then import your CA certificates into the root trust database of your managed machines.

If you're using a self-signed certificate, consider using a self-signed CA to sign a CSR for your service usage, then import the public certificate of your CA into the System keychain on all client computers (if you have control of the computers).

Using Certificate Manager

Leopard Server's Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services.

The Server Admin interface is shown below, with the Certificate Manager selected.



Certificate Manager provides integrated management of SSL certificates in Leopard Server for services that allow the use of SSL certificates.

Certificate Manager allows you to create self-signed certificates and obtain certificates signed by a CA. The certificates, self-signed or signed by a CA, are accessible by the services that support SSL.

Identities that were created and stored in OpenSSL files can also be imported into Certificate Manager. They are accessible to services that support SSL.

Certificate Manager in Server Admin doesn't allow you to sign and issue certificates as a CA, nor does it allow you to sign and issue certificates as a root authority. If you need these functions, you can use CA Assistant in Keychain Access (located in /Applications/Utilities/). It provides these capabilities and others for working with x.509 certificates.

Self-signed and CA-issued certificates you create in CA Assistant can be used in Certificate Manager by importing the certificate.

Certificate Manager displays the following for each certificate:

- The domain name that the certificate was issued for
- The dates of validity
- The signing authority (such as the CA entity, or if the certificate is self-signed, it reads "Self-Signed")

Requesting a Certificate from a CA

Certificate Manager helps you create a CSR to send to your designated CA.

To request a signed certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Below the Certificates list click the Add (+) button.
4. Fill out identity information.

 The common name is the fully qualified domain name of the server that will use SSL-enabled services.
5. Enter starting and ending validity dates.
6. Select a private key size.

 The default is1024 bits.
7. Enter a passphrase for the private key.

 This passphrase should be more secure than a normal password.

 It is recommended you use at least 20 characters. Include mixed case, numbers, and punctuation; do not repeat characters; do not use dictionary terms.
8. Click the Gear button and choose "Generate Certificate Signing Request."
9. Follow the onscreen directions for requesting a signed certificate from your CA.

 For example, you might need to do it online or enter a mail address.
10. Click Send Request.
11. Click Done to save the identity information.

 When the CA replies to the mail, the CA includes the certificate in the text of the reply.
12. Make sure the Certificate is selected in the Certificates field again.
13. Click the Gear button, then choose Add Signed or Renewal Certificate from Certificate Authority.
14. Copy the characters from "==Begin CSR==" to "==End CSR==" into the text box.
15. Click OK.
16. Click Save.

Creating a Self-Signed Certificate

When you create an identity in Certificate Manager, you're creating a self-signed certificate. Certificate Manager creates a private–public key pair in the system keychain with the key size specified (512–2048 bits). It then creates the corresponding self-signed certificate in the system keychain.

A CSR is also generated at the same time that the self-signed certificate is created. This isn't stored in the keychain but is written to disk at /etc/certificates/cert.common.name.tld.csr, where common.name.tld is the common name of the certificate that was issued.

To create a self-signed certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Click the Add (+) button.
4. Fill out identity information.

 The common name is the fully qualified domain name of the server that will use SSL-enabled services.
5. Enter starting and ending validity dates.
6. Select a private key size (1024 bits is the default).
7. Enter a passphrase for the private key.

 This passphrase should be more secure than a normal password.

 It is recommended you use at least 20 characters. Include mixed case, numbers, and punctuation; do not repeat characters; do not use dictionary terms.
8. Click Done to save the identity information.
9. Click Save.

Importing a Certificate

You can import a previously generated OpenSSL certificate and private key into Certificate Manager. The items are listed as available in the list of identities and are available to SSL-enabled services.

To import an OpenSSL certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Click the Import button.
4. Enter the existing certificate's file name and path.

 Alternatively, browse for its location.

5 Enter the existing private key file's name and path.

Alternatively, browse for its location.

6 Enter the private key passphrase.

7 Click Import.

Managing Certificates

After you create and sign a certificate, you won't do much more with it. You can use Server Admin to edit certificates before a CA signs them. Except for self-signed certificates, you cannot change certificates after a CA signs them.

If the information a certificate possesses (such as contact information) is no longer accurate, or if you believe the private key is compromised, delete the certificate.

Editing a Certificate

After you add a certificate signature, you can't edit the certificate. However, you can edit a self-signed certificate. You can modify all fields, including domain name and private key passphrase, private key size, and so forth.

If the identity was exported to disk from the system keychain, re-export it.

To edit a certificate:

1 In Server Admin, select the server that has services that support SSL.

2 Click Certificates.

3 Select the Certificate Identity to edit.

It must be a self-signed certificate.

4 Click the Edit (/) button.

5 Click Edit.

Deleting a Certificate

When a certificate has expired or been compromised, delete it.

To delete a certificate:

1 In Server Admin, select the server that has services that support SSL.

2 Click Certificates.

3 Select the Certificate Identity to delete.

4 Click the Remove (–) button and select Delete.

5 Click Save.

Renewing an Expiring Certificate

All certificates have an expiration date and must be updated periodically.

To renew an expiring certificate:

1. Request a new certificate from the CA.

 If you are your own CA, create a certificate one using your own root certificate.
2. In Server Admin in the Server list, select the server that has the expiring certificate.
3. Click Certificates.
4. Select the Certificate Identity to edit.
5. Click the action button and select "Add signed or renewed certificate from certificate authority."
6. Paste the renewed certificate into the text field and click OK.
7. Click the Edit button to make the certificate editable.
8. Adjust the dates for the certificate.
9. Click Save.

Creating a CA

If your server must communicate using SSL with external computers out of your control, purchase SSL certificates from a well-known CA. After you obtain the certificates, configuration of the services is the same whether they were purchased from a vendor or signed by your own CA.

If you are setting up an internal network and only need to encrypt local traffic, set up a CA to sign SSL certificates for the internal network. The next sections describe this process.

Although the security is only as good as the security of the CA, in many cases this is sufficient to enable encrypted communication between a web or mail server and their clients. The basic steps to set up an internal SSL-encrypted network are:

1. Create a CA.
2. Distribute the CA's certificate to client systems.
3. Use the CA to sign the certificates the servers will use.

Creating a CA Using Certificate Assistant

To sign another user's certificate, you must create a CA. Sometimes a CA certificate is referred to as a root certificate. By signing a certificate with the root certificate, you become the trusted third party in that certificate's transactions, vouching for the identity of the certificate holder.

If you are a large organization, you might decide to issue or sign certificates for people in your organization to use the security benefits of certificates. However, external organizations might not trust or recognize your signing authority.

Because the security of your certificates relies on the security of the CA, performing these steps on a secure computer is critical. The computer should be physically secure and not connected to a network.

To create a CA:

1. Start Keychain Access.

 Keychain Access is found in the /Applications/Utilities/ directory.

2. In the Keychain Access menu, select Certificate Assistant > Create a Certificate Authority.

 The Certificate Assistant starts, and guides you through the process of making the CA.

3. Choose to create a Self Signed Root CA.

4. Provide the Certificate Assistant with the requested information and click Continue.

 You need the following information to create a CA:

 - A mail address
 - The name of the issuing authority (you or your organization)

 You also decide if you want to override the defaults and whether to make this CA the organization's default CA. If you do not have a default CA for the organization, allow the Certificate Assistant to make this CA the default.

 In most circumstances, you do not want to override the defaults. If you do not override the defaults, skip to step 16.

5. If you choose to override the defaults, provide the following information in the next few screens:

 - A unique serial number for the root certificate
 - The number of days the CA functions before expiring
 - The type of user certificate this CA is signing
 - Whether to create a CA website for users to access to distribute CA certificates

6. Click Continue.

7. Provide the Certificate Assistant with the requested information and click Continue.

 You need the following information to create a CA:

 - A mail address of the responsible party for certificates
 - The name of the issuing authority (you or your organization)
 - The organization name
 - The organization unit name
 - The location of the issuing authority

8. Select a key size and an encryption algorithm for the CA certificate and then click Continue.

 A larger key size is more computationally intensive to use, but much more secure. The algorithm you choose depends more on your organizational needs than a technical consideration. DSA and RSA are strong encryption algorithms. DSA is a United States Federal Government standard for digital signatures. RSA is a more recent advance in algorithms.

9. Select a key size and an encryption algorithm for the certificates to be signed and click Continue.
10. Select the Key Usage Extensions you need for the CA certificate and click Continue.

 At a minimum, you must select Signature and Certificate Signing.

11. Select the Key Usage Extensions you need for the certificates to be signed and click Continue.

 Default key use selections are based on the type of key selected earlier in the Assistant.

12. Specify other extensions to add the CA certificate and click Continue.

 You must select "Include Basic Constraints" and "Use this certificate as a certificate authority"

13. Specify other extensions to add to the CA certificate and click Continue.

 No other extensions are required.

14. Select the keychain "System" to store the CA certificate.
15. Choose to trust certificates on this computer signed by the created CA.
16. Click Continue and authenticate as an administrator to create the certificate and key pair.
17. Read and follow the instructions on the last page of the Certificate Assistant.

 You can now issue certificates to trusted parties and sign CSRs.

Creating a CA from the Command Line

Because the security of your certificates relies on the security of the CA, performing these steps on a secure computer is critical. The computer should be physically secure and not connected to a network.

To create the CA using the openssl command:

1. Enter the following in Terminal to create a certificate directory.

```
$ cd /usr/share
$ sudo mkdir certs
$ cd certs
```

2. Generate a key pair with the `openssl` command.

```
$ sudo openssl genrsa -des3 -out ca.key 2048
```

This command generates a Triple-DES encrypted RSA public-private key pair names ca.key. The `2048` is the length of the key in bits. OpenSSL asks for a passphrase for the key upon creating it. Use a strong passphrase and keep it secure. A compromise of this passphrase undermines the security of your entire certificate system.

Create a Certificate for Someone Else

You can use your CA certificate to issue a certificate to someone else. By doing so you are stating you are a trusted party and can verify the identity of the certificate holder.

Before you can create a certificate for someone, that person must generate a CSR. The user can use the Certificate Assistant to generate the CSR and mail the request to you. You then use the CSR's text to make the certificate.

To create a certificate for someone else:

1. Start Keychain Access.

 Keychain Access is found in the /Applications/Utilities/ directory.

2. In the Keychain Access menu, select Certificate Assistant > Create a Certificate for Someone Else as a Certificate Signing Authority.

 The Certificate Assistant starts, and guides you through the process of making the CA.

3. Drag the CSR and drop it on the target area.

4. Choose the CA that is the issuer and sign the request.

 Also, you can choose to override the request defaults.

5. Click Continue.

 If you override the request defaults, provide the Certificate Assistant with the requested information and click Continue.

 The Certificate is now signed. The default mail application launches with the signed certificate as an attachment.

Storing the CA Private Key

The CA private key should be generated on a computer that is not connected to your internal network. For added security, you can store the keychain containing the private key on USB storage so you can keep the CA private key unavailable when connected to the network.

Creating Folders and Files for SSL

When signing certificates, SSL looks for keys and related information in directories specified in its configuration file, openssl.cnf, which is found in /System/Library/OpenSSL/.

To create directories and files where SSL expects to find them by default:

```
$ cd /usr/share/certs
$ sudo -s
$ mkdir -p demoCA/private
$ cp ca.key demoCA/private/cakey.pem
$ cp ca.crt demoCA/cacert.pem
$ mkdir demoCA/newcerts
$ touch demoCA/index.txt
$ echo "01" > demoCA/serial
$ exit
```

The CA can now sign certificates for servers, enabling encrypted communication between servers and clients.

Distributing a CA Public Certificate to Clients

If you're using self-signed certificates, a warning appears in most user applications saying that the CA is not recognized. Other software, such as the LDAP client, refuses to use SSL if the server's CA is unknown.

Leopard Server ships only with certificates from well-known commercial CAs. To prevent this warning, your CA certificate must be distributed to every client computer that connects to the secure server.

To distribute the self-signed CA certificate:

1. Copy the self-signed CA certificate (the file named ca.crt) onto each client computer.

 This is preferably distributed using nonrewritable media, such as a CD-R. Using nonrewritable media prevents the certificate from being corrupted.

2. Open the Keychain Access tool by double-clicking the ca.crt icon where the certificate was copied onto the client computer.

3. Add the certificate to the System keychain using Keychain Access.

 Alternatively, use the `certtool` command in Terminal:

   ```
   sudo certtool i ca.crt k=/System/Library/Keychains/Systems
   ```

 As a result, any client application (such as Safari or Mail) that verifies certificates using the System keychain recognizes certificates signed by your CA.

Setting General Protocols and Access to Services

13

Use this chapter to learn how to use Server Admin to configure access to services and to set general protocols.

Server Admin helps you configure and manage your servers. Using Server Admin, you can set general protocols, name or rename computers, set the date and time, manage certificates, and set user access to specific services.

Setting General Protocols

Leopard Server includes basic network management protocols, including network time protocol (NTP) and simple network management protocol (SNMP). Unless these are required, they should be disabled.

Configuring NTP

The NTP software allows computers on a network to synchronize their Date & Time settings. Client computers specify their NTP server in the Date & Time panel of System Preferences.

NTP is typically required. If so, enable it on a single, trusted server on the local network. This service should be disabled on all other servers.

For more information about the open source implementation, see www.ntp.org.

To configure NTP service:

1. Open Server Admin and connect to the server.
2. Click Settings, then click Date & Time.
3. Unless NTP is not required, make sure your server is configured to "Set date & time automatically."
4. From the pop-up menu, choose the server you want to act as a time server.
5. Click General.
6. If NTP is not required, deselect the "Network Time Server (NTP)" checkbox.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Setting General Protocols
# ------------------------------------------------------------------

# Disable NTP
# -----------
systemsetup -setusingnetworktime off
```

Disabling SNMP

SNMP software allows other computers to monitor and collect data on the state of a computer running Leopard Server. This helps administrators identify computers that warrant attention, but use of this service is not recommended.

To disable SNMP:

1. Open Server Admin and connect to the server.
2. Click Settings.
3. Click General.
4. Deselect "Enable NTP" and "Enable SNMP."
5. Click Save.

From the Command Line:

```
# Disable SNMP
# ------------
service org.net-snmp.snmpd stop
```

Enabling SSH

Leopard Server also includes secure shell (SSH). SSH allows you to log in to other computers on a network, execute commands remotely, and move files from one computer to another. It provides strong authentication and secure communication, and is therefore recommended if remote login is required. For more information, see www.openssh.org.

To enable SSH:

1. Open Server Admin and connect to the server.
2. Click Settings.
3. Click General.
4. Select "Enable SSH (required while creating an Open Directory replica)."
5. Click Save.

From the Command Line:

```
# Enable SSH
# ----------
service ssh start
```

Remote Management (ARD)

You can use Apple Remote Desktop (ARD) to perform remote management tasks such as screen sharing. When sharing your screen you should provide access to specific users to prevent unauthorized access to your computer screen. You also need to determine the privileges users will have when viewing your screen.

An ARD manager with full privileges can run these tasks as the root user. By limiting the privileges that an ARD manager has, you can increase security. When setting privileges, disable or limit an administrator's access to an ARD client.

You can set a VNC password that requires authorized users to use a password to access your computer. The most secure way is to require authorized users to request permission to access your computer screen.

ARD is turned off by default and should remain off when it is not being used. This prevents unauthorized users from attempting to access your computer.

Restricting Access to Specific Users

If you need to share your screen using ARD, you must securely turn on remote management in Sharing preferences.

The default setting for remote management should be changed from "All users" to "Only these users." The default setting "All users" includes all users on your local computer and all users in the directory server you are connected to.

Any account using ARD should have limited privileges to prevent remote users from having full control of your computer.

You can securely configure ARD by restricting access to specific users. You can also restrict each user's privileges by setting ARD options. The user's privileges should be limited to the user's permission on the computer. For example, you might not want to give a standard user the ability to change your settings or delete items.

For more information, see *Apple Remote Desktop Administration Guide*.

You can also securely configure computer settings for remote management. If users connect to your computer using VNC, require that they use a password by enabling "VNC viewer may control screen with password." Use Password Assistant to create a strong password for VNC users.

From the Command Line:

```
# Remote Management (ARD)
# ---------------------------
# Disable Remote Management.
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
     Resources/kickstart -deactivate -stop
```

Remote Apple Events (RAE)

If you enable Remote Apple Events (RAE), you allow your computer to respond to events sent by other computers on your network. These events include AppleScript programs. A malicious AppleScript program can do things like delete your ~/Documents/ folder.

RAE is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

From the Command Line:

```
# Remote Apple Events (RAE)
# ---------------------------
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist
```

Restricting Access to Specific Users

Avoid enabling RAE. If you enable RAE, do so on a trusted private network and disable it immediately after disconnecting from the network. The default setting for RAE should be changed from "All users" to "Only these users." The default setting "All users" includes all users on your local computer and all users in the directory server you are connected to.

When securely configuring RAE, restrict remote events to only be accepted from specific users. This prevents unauthorized users form sending malicious events to your computer. If you create a sharing user account, create a strong password using Password Assistant. Avoid accepting events from Mac OS 9 computers. If you need to accept Mac OS 9 events, use Password Assistant to create a strong password.

Setting the Server's Host Name

You can change your computer name and local host name in Server Admin. When other users use Bonjour to discover your available services, the server is displayed as *hostname*.local.

To increase your privacy, change the host name of your computer so your computer cannot be easily identified. The name should not indicate the purpose of the computer and the word "server" should not be used as the name or part of the name.

Setting the Date and Time

Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues. You can use Server Admin to configure your computer to set the date and time based on an NTP server. If you require automatic date and time, use a trusted, internal NTP server.

Setting Up Certificates

Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services. Certificate Manager provides integrated management of SSL certificates in Leopard Server for services that allow the use of SSL certificates.

For more information about setting up certificates, see "Obtaining Certificates" on page 191.

Setting Service Access Control Lists

You use a Service Access Control List (SACL) to enforce who can use a specific service. It is not a means of authentication. It is a list of those who have access rights to use the service.

SACLs allow you to add a layer of access control on top of standard and ACL permissions.

A user or group not in a service's SACL cannot access the service. For example, to prevent users from accessing AFP share points on a server, including home folders, remove the users from the AFP service's SACL.

Server Admin in Leopard Server allows you to configure SACLs. Open Directory authenticates user accounts, and SACLs authorize use of services. If Open Directory authenticates you, the SACL for the login window determines whether you can log in, the SACL for AFP service determines whether you can connect for Apple file service, and so on.

Some services also determine whether a user is authorized to access specific resources. This authorization can require retrieving additional user account information from the directory domain. For example, AFP service needs the user ID and group membership information to determine which folders and files the user is authorized to read and write.

To set SACL permissions for a service:

1. Open Server Admin.
2. Select the server from the Servers list.
3. Click Settings.
4. Click Access.
5. To restrict access to all services or to deselect this option to set access permissions per service, select "For all services."
6. If you deselect "For all services," select a service from the Service list.
7. To provide unrestricted access to services, click "Allow all users and groups."

 To provide access to specific users and groups:

 a. Select "Allow only users and groups below."
 b. Click the Add (+) button to open the Users & Groups drawer.
 c. Drag users and groups from the Users & Groups drawer to the list.
8. Click Save.

You can limit access to command-line tools that might run services by limiting the use of the `sudo` command. For more information, see "Managing the sudoers File" on page 369.

From the Command Line:

```
# Set SACL permissions for a service
# ---------------------------------
dseditgroup -o edit -a $USER -t user $SACL_GROUP
```

Securing Remote Access Services

14

Use this chapter to learn how to secure Remote Access services.

Many organizations have individuals who need to connect to network resources remotely. This can create additional vulnerabilities unless your remote access services are securely configured.

Leopard Server allows remote access using remote login and VPN services. These services should be disabled unless they are required.

Remote Access services via remote login consists of two components each using the Secure Shell (SSH) service to establish an encrypted tunnel between client and server. "Securing Remote Login (SSH)" on page 207 discusses securing the server component, while "Configuring Secure Shell" on page 208 discusses securing the client component.

For additional information about configuring remote access services, see the *Network Services Administration* guide.

Securing Remote Login (SSH)

Remote Login allows users to connect to your computer through SSH. By enabling Remote Login, you activate more secure versions of commonly used insecure tools.

Be aware of the following SSH tools:

- `sshd`—Daemon that acts as a server to all other commands
- `ssh`—Primary user tool: remote shell, remote command, and port-forwarding sessions
- `scp`—Secure copy, a tool for automated file transfers
- `sftp`—Secure FTP, a replacement for FTP

The following table lists tools enabled with Remote Login and their insecure counterparts.

Secure Remote Login Tool	Insecure Tool
ssh	telnet
slogin	login
scp	rcp
sftp	ftp

SSH creates a secure encrypted channel that protects communication with your computers. Older services that do not encrypt their communications, such as Telnet or RSH, should never be used—they allow network eavesdroppers to intercept passwords or other data.

Unless you must remotely log in to the computer or use another program that depends on SSH, disable the remote login service. However, Server Admin requires that you enable SSH. If you disable remote login, you cannot use Server Admin to remotely administer the server.

To disable remote login:

1. Open System Preferences.
2. Click Sharing.
3. In the Service list deselect Remote Login.

Configuring Secure Shell

SSH lets you send secure, encrypted commands to a remote computer, as if you were sitting at the computer. Use the `ssh` tool in Terminal to open a command-line connection to a remote computer. While the connection is open, commands you enter are performed on the remote computer.

Note: You can use any application that supports SSH to connect to a computer running Leopard or Leopard Server.

SSH works by setting up encrypted tunnels using public and private keys. Here is a description of an SSH session:

1. The local and remote computers exchange their public keys.

 If the local computer has never encountered a given public key before, SSH prompts you whether to accept the unknown key.
2. The two computers use the public keys to negotiate a session key that is used to encrypt subsequent session data.

3 The remote computer attempts to authenticate the local computer using RSA or DSA certificates. If this is not possible, the local computer is prompted for a standard user-name/password combination.

For information about setting up certificate authentication, see "Generating Key Pairs for Key-Based SSH Connections" on page 209.

4 After successful authentication, the session begins. Either a remote shell, a secure file transfer, a remote command, or so on, begins through the encrypted tunnel.

Modifying the SSH Configuration File

Making changes to the SSH configuration file enables you to set options for each ssh connection. You can make these changes systemwide or for specific users. To make the change systemwide, change the options in the /etc/ssh_config file, which affects ssh users on the computer. To make the change for a single user, change the options in the *username*/.ssh/config file.

The ssh configuration file has connection options and other specifications for an ssh host. A host is specified by the Host declaration. By default, the Host declaration is an asterisk (*), indicating that any host you are connecting to will use the options listed below the Host declaration.

You can add a specific host and options for that host by adding a new Host declaration. The new Host declaration will specify a name or address in place of the asterisk. You can then set the connection option for you new host below the Host declaration. This helps secure your ssh sessions in environments with varying security levels.

For example, if you are connecting to a server using ssh through the Internet, the server might require a more secure or stricter connection options. However, if you are in a more secure environment, such as your own personal network, you cannot require the same strict connection options.

For more information about ssh configuration file options, see the ssh man pages.

To enable SSH, see "Enabling SSH" on page 202.

Generating Key Pairs for Key-Based SSH Connections

By default, SSH supports the use of password, key, and Kerberos authentication. The standard method of SSH authentication is to supply login credentials in the form of a user name and password. Identity key pair authentication enables you to log in to the server without supplying a password.

This process works as follows:

1 A private and a public key are generated, each associated with a user name to establish that user's authenticity.

2 When you attempt to log in as that user, the user name is sent to the remote computer.

3 The remote computer looks in the user's .ssh/ folder for the user's public key.

This folder is created after using SSH the first time.

4 A challenge is then sent to the user based on his or her public key.

5 The user verifies his or her identity by using the private portion of the key pair to decode the challenge.

6 After the challenge is decoded, the user is logged in without the need for a password.

This is especially useful when automating remote scripts.

Key-based authentication requires possession of the private key instead of a password in order to log in to the server. A private key is much harder to guess than a password. However, if the home folder in which the private key is stored is compromised—assuming the private key is not protected by a password—then this private key could be used to log in to other systems. Password authentication can be compromised without needing a private key file.

If the server uses FileVault to encrypt the home folder of the user you want to use SSH to connect as, you must be logged in on the server to use SSH. Alternatively, you can store the keys for the user in a location that is not protected by FileVault. However, this is not secure.

To generate the identity key pair:

1 Enter the following command on the local computer.

```
$ ssh-keygen -t dsa
```

2 When prompted, enter a filename to save the keys in the user's folder.

3 Enter a password followed by password verification (empty for no password).

For example:

```
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/anne/.ssh/id_dsa): frog
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in frog.
Your public key has been saved in frog.pub.
The key fingerprint is:
4a:5c:6e:9f:3e:35:8b:e5:c9:5a:ac:00:e6:b8:d7:96 annejohnson1@mac.com
```

This creates two files. Your identification or private key is saved in one file (frog in our example) and your public key is saved in the other (frog.pub in our example). The key fingerprint, which is derived cryptographically from the public key value, is also displayed. This secures the public key, making it computationally infeasible for duplication.

Note: The location of the server SSH key is /etc/ssh_host_key.pub. Back up your key in case you need to reinstall your server software. If your server software is reinstalled, you can retain the server identity by putting the key back in its folder.

4 Copy the resultant public file, which contains the local computer's public key, to the .ssh/ folder in the user's home folder on the remote computer.

The next time you log in to the remote computer from the local computer, you won't need to enter a password (unless you entered one in Step 3 above).

Note: If you are using an Open Directory user account and have logged in using the account, you do not need to supply a password for SSH login. On Leopard Server computers, SSH uses Kerberos for single sign-on authentication with any user account that has an Open Directory password (but Kerberos must be running on the Open Directory server). For more information see the *Open Directory Administration* guide.

Updating SSH Key Fingerprints

The first time you connect to a remote computer using SSH, the local computer prompts for permission to add the remote computer's fingerprint (or encrypted public key) to a list of known remote computers. You might see a message like this:

```
The authenticity of host "server1.example.com" can't be established.
RSA key fingerprint is a8:0d:27:63:74:f1:ad:bd:6a:e4:0d:a3:47:a8:f7.
Are you sure you want to continue connecting (yes/no)?
```

The first time you connect, you have no way of knowing whether this is the correct host key. When you respond "yes," the host key is then inserted into the ~/.ssh/known_hosts file so it can be compared in later sessions. Be sure this is the correct key before accepting it. If at all possible, provide your users with the encryption key through FTP, mail, or a download from the web, so they can verify the identity of the server.

If you later see a warning message about a man-in-the-middle attack when you try to connect, the key on the remote computer might no longer match the key stored on the local computer. This can happen if you:

- Change your SSH configuration on the local or remote computer.
- Perform a clean installation of the server software on the computer you are attempting to log in to using SSH.
- Start up from a Leopard Server CD on the computer you are attempting to log in to using SSH.
- Attempt to use SSH to log in to a computer that has the same IP address as a computer that you previously used SSH with on another network.

To connect again, delete the entries corresponding to the remote computer you are accessing (which can be stored by both name and IP address) in ~/.ssh/known_hosts.

Important: Removing an entry from the known_hosts file bypasses a security mechanism that helps you avoid imposters and man-in-the-middle attacks. Be sure you understand why the key on the remote computer has changed before you delete its entry from the known_hosts file.

Controlling Access to SSH

You can use Server Admin to control which users can open a command-line connection using the `ssh` tool in Terminal. Users with administrator privileges are always allowed to open a connection using SSH. The `ssh` tool uses the SSH service.

For information about restricting user access to services, see "Setting Service Access Control Lists" on page 205.

SSH Man-in-the-Middle Attacks

An attacker might be able to get access to your network and compromise routing information, so that packets intended for a remote computer are routed to the attacker who impersonates the remote computer to the local computer and the local computer to the remote computer.

Here's a typical scenario: A user connects to the remote computer using SSH. By means of spoofing techniques, the attacker poses as the remote computer and receives the information from the local computer. The attacker then relays the information to the intended remote computer, receives a response, and then relays the remote computer's response to the local computer. Throughout the process, the attacker is aware of all the information that goes back and forth, and can modify it.

The following message can indicate a man-in-the-middle attack when connecting to the remote computer using SSH.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

Protect against this type of attack by verifying that the host key sent back is the correct host key for the computer you are trying to reach. Be watchful for the warning message, and alert your users to its meaning.

Transferring Files Using SFTP

SFTP is a secure FTP protocol that uses SSH to transfer files. SFTP encrypts commands and data, preventing passwords and sensitive information from being transmitted over the network. SFTP should always be used instead of FTP.

To transfer a file using SFTP:

1. Open Terminal.
2. Start the SFTP session.

   ```
   $ sftp username@hostname
   ```

 Replace *username* with your user name and *hostname* with the IP address or host name of the server you are connecting to.
3. Enter your password when prompted.

 You are now connected securely to the server.
4. Use the SFTP commands to transfer files from the prompt.

   ```
   sftp>
   ```

 Use the `put` command to transfer a file from the local computer to the remote computer. Use the `get` command to transfer a file from the remote computer to the local computer.
5. Enter the following to transfer a picture file from the remote computer to the local computer.

   ```
   sftp> get picture.png /users/annejohnson picture.png
   ```
6. To disconnect and end the SFTP session, enter `exit` at the prompt.

Securing VPN Service

By configuring a Virtual Private Network (VPN) on your server, you can give users a more secure way of remotely communicating with computers on your network.

A VPN consists of computers or networks (nodes) connected by a private link of encrypted data. This link simulates a local connection, as if the remote computer were attached to the local area network (LAN).

VPNs securely connect users working away from the office (for example, at home) to the LAN through a connection such as the Internet. From the user's perspective, the VPN connection appears as a dedicated private link.

VPN technology can also connect an organization to branch offices over the Internet while maintaining secure communications. The VPN connection across the Internet acts as a wide area network (WAN) link between the sites.

VPNs have several advantages for organizations whose computer resources are physically separated. For example, each remote user or node uses the network resources of its Internet Service Provider (ISP) rather than having a direct, wired link to the main location.

VPN and Security

VPNs increase security by requiring strong authentication of identity and encrypted data transport between the nodes for data privacy and dependability. The following sections contain information about supported transports and authentication methods.

Transport Protocols

There are two encrypted transport protocols: Layer Two Tunneling Protocol, Secure Internet Protocol (L2TP/IPSec) and Point–to–Point Tunneling Protocol (PPTP). You can enable either or both of these protocols. Each has its own strengths and requirements.

L2TP/IPSec

L2TP/IPSec uses strong IPSec encryption to tunnel data to and from network nodes. It is based on Cisco's L2F protocol.

IPSec requires security certificates (self-signed or signed by a CA such as Verisign) or a predefined shared secret between connecting nodes.

The shared secret must be entered on the server and the client.

The shared secret is not a password for authentication, nor does it generate encryption keys to establish secure tunnels between nodes. It is a token that the key management systems use to trust each other.

L2TP is Leopard Server's preferred VPN protocol because it has superior transport encryption and can be authenticated using Kerberos.

PPTP

PPTP is a commonly used Windows standard VPN protocol. PPTP offers good encryption (if strong passwords are used) and supports a number of authentication schemes. It uses the user-provided password to produce an encryption key.

By default, PPTP supports 128-bit (strong) encryption. PPTP also supports the 40-bit (weak) security encryption.

PPTP is necessary if you have Windows clients with versions earlier than Windows XP or if you have Mac OS X v10.2 clients or earlier.

Configuring L2TP/IPSec Settings

Use Server Admin to designate L2TP as the transport protocol. If you enable this protocol, you must also configure connection settings. You must designate an IPSec shared secret (if you don't use a signed security certificate), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed). If you use L2TP and PPTP, provide each protocol with a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the "any" address group, enable GRE, ESP, VPN L2TP (port 1701), and VPN ISAKMP/IKE (port 500).
- For the "192.168-net" address group, choose to allow all traffic.

To configure L2TP settings:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click L2TP.
5. Select the "Enable L2TP over IPSec" checkbox.
6. In the "Starting IP address" field, set the beginning IP address of the VPN allocation range.

 It can't overlap the DHCP allocation range, so enter 192.168.0.128.
7. In the "Ending IP address" field, set the ending IP address of the VPN allocation range.

 It can't overlap the DHCP allocation range, so enter 192.168.0.255.
8. (Optional) You can load-balance the VPN by selecting the Enable Load Balancing checkbox and entering an IP address in the Cluster IP address field.
9. Choose a PPP authentication type.

 If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

 If you choose RADIUS, enter the following information:

 Primary IP Address: Enter the IP address of the primary RADIUS server.

 Shared Secret: Enter a shared secret for the primary RADIUS server.

 Secondary IP Address: Enter the IP address of the secondary RADIUS server.

 Shared Secret: Enter a shared secret for the secondary RADIUS server.

10 In the IPSec Authentication section enter the shared secret or select the certificate to use.

The shared secret is a common password that authenticates members of the cluster. IPSec uses the shared secret as a preshared key to establish secure tunnels between cluster nodes.

11 Click Save.

Configuring PPTP Settings

Use Server Admin to designate PPTP as the transport protocol.

If you enable this protocol, you must also configure connection settings. You should designate an encryption key length (40-bit or 128-bit), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed).

If you use L2TP and PPTP, provide protocol with a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the "any" address group, enable GRE, ESP, VPN L2TP (port 1701), and IKE (port 500).
- For the "192.168-net" address group, choose to allow all traffic.

To configure PPTP settings:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click Settings, then click PPTP.

5 Select "Enable PPTP."

6 If needed, select "Allow 40-bit encryption keys in addition to 128-bit" to permit both 40-bit and 128-bit key encryption access to VPN.

> *WARNING:* 40-bit encryption keys are much less secure but can be necessary for some VPN client applications.

7 In the "Starting IP address" field, set the beginning IP address of the VPN allocation range.

It can't overlap the DHCP allocation range, so enter 192.168.0.128.

8 In the "Ending IP address" field, set the ending IP address of the VPN allocation range.

It can't overlap the DHCP allocation range, so enter 192.168.0.255.

9 Choose a PPP authentication type.

If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

If you choose RADIUS, enter the following information:

Primary IP Address: Enter the IP address of the primary RADIUS server.

Shared Secret: Enter a shared secret for the primary RADIUS server.

Secondary IP Address: Enter the IP address of the secondary RADIUS server.

Shared Secret: Enter a shared secret for the secondary RADIUS server.

10 Click Save.

Authentication Method

Leopard Server L2TP VPN uses Kerberos v5 or Microsoft's Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) for authentication. Leopard Server PPTP VPN uses MS-CHAPv2 for authentication.

Kerberos is a secure authentication protocol that uses a Kerberos Key Distribution Server as a trusted third party to authenticate a client to a server.

MS-CHAPv2 authentication encodes passwords when they're sent over the network, and stores them in a scrambled form on the server. This method offers good security during network transmission. It is also the standard Windows authentication scheme for VPN.

Leopard Server PPTP VPN can also use other authentication methods. Each method has its own strengths and requirements. These other authentication methods for PPTP are not available in Server Admin.

If you want to use an alternative authentication scheme (for example, to use RSA Security's SecurID authentication), you must edit the VPN configuration file manually. The configuration file is located at /Library/Preferences/SystemConfiguration/com.apple.RemoteAccessServers.plist.

For more information, see "Offering SecurID Authentication with VPN Service" on page 218.

Using VPN Service with Users in a Third-Party LDAP Domain

To use VPN service for users in a third-party LDAP domain (an Active Directory or Linux OpenLDAP domain), you must be able to use Kerberos authentication. If you need to use MSCHAPv2 to authenticate users, you can't offer VPN service for users in a third-party LDAP domain.

Offering SecurID Authentication with VPN Service

RSA Security provides strong authentication. They use hardware and software tokens to verify user identity. SecurID authentication is available for L2TP and PPTP transports. For details and product offerings, see www.rsasecurity.com.

Leopard Server VPN service can offer SecurID authentication, but it cannot be set up in Server Admin. You can use Server Admin to configure standard VPN services, but Server Admin does not have an interface for choosing your authentication method. If you must designate an authentication scheme (such as RSA Security SecurID) other than the default, change the VPN configuration manually. For additional information, see the *RSA SecurID Ready Implementation Guide,* located on the web at rsasecurity.agora.com/rsasecured/guides/imp_pdfs/MacOSX_ACE_51.pdf.

To manually configure RSA Security SecurID authentication:

1. Open Terminal.
2. Create a folder named /var/ace on your Leopard Server.

   ```
   $ sudo mkdir /var/ace
   ```

 Authenticate, if requested.
3. In Finder, choose Go > Go to Folder.
4. Type `/var/ace`.
5. Click Go.
6. Copy the sdconf.rec file from a SecurID server to /var/ace/.

 You will see a dialog indicating that the /var/ace/ folder cannot be modified. Click Authenticate to allow the copy.
7. Configure the VPN service (PPTP or L2TP) on your Leopard Server to enable EAP-SecurID authentication for the protocols you want to use it with.

 Enter the following in Terminal, replacing *`protocol`* with either `pptp` or `l2tp`:

   ```
   $ sudo serveradmin settings
        vpn:Servers:com.apple.ppp.protocol:PPP:AuthenticatorEAPPlugins:_array_i
        ndex : 0 = "EAP-RSA"
   $ sudo serveradmin settings
        vpn:Servers:com.apple.ppp.protocol:PPP:AuthenticatorProtocol:_array_ind
        ex: = "EAP"
   ```

 The remainder of Leopard Server VPN service configuration can be done using the Server Admin application.

Encrypting Observe and Control Network Data

Although Remote Desktop sends authentication information, keystrokes, and management commands encrypted by default, you might want additional security. You can choose to encrypt all Observe and Control traffic, at a performance cost.

Encryption is done using an SSH tunnel between participating computers. To use encryption for Observe and Control tasks, the target computers must have SSH enabled ("Remote Login" in the computer's Sharing Preference pane). Additionally, firewalls between the participating computers must be configured to pass traffic on TCP port 22 (SSH well known port).

If the you are trying to control a VNC server that is not a remote desktop, it cannot support Remote Desktop keystroke encryption. If you try to control that VNC server, you get a warning that the keystrokes aren't encrypted, which you must acknowledge before you can control the VNC server. If you chose to encrypt all network data, then you cannot control the VNC server because Remote Desktop cannot open the necessary SSH tunnel to the VNC server.

To enable Observe and Control transport encryption:

1. Choose Remote Desktop > Preferences.
2. Click the Security button.
3. In the "Controlling computers" section, select "Encrypt all network data."

Encrypting Network Data During File Copy and Package Installations

Remote Desktop can send files for Copy Items and Install Packages via encrypted transport. This option is not enabled by default, and you must enable it explicitly for each copy task, or in a global setting in Remote Desktop's preferences. Even installer package files can be intercepted if not encrypted.

To encrypt individual file copying and package installation tasks:

- In the Copy Items task or Install Packages task configuration window, select "Encrypt network data."

To set a default encryption preference for file copies:

1. In the Remote Desktop Preferences window, select the Security pane.
2. Select "Encrypt transfers when using Copy Items," or "Encrypt transfers when using Install Packages" as needed.

Alternatively, you could encrypt a file archive before copying it. The encrypted archive could be intercepted, but it would be unreadable.

Remote Apple Events (RAE)

If you enable Remote Apple Events (RAE), you allow your computer to respond to events sent by other computers on your network. These events include AppleScript programs. A malicious AppleScript program can do things like delete your ~/Documents/ folder.

RAE is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

From the Command Line:

```
# Remote Apple Events (RAE)
# -----------------------------
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist
```

Restricting Access to Specific Users

Avoid enabling RAE. If you enable RAE, do so on a trusted private network and disable it immediately after disconnecting from the network. The default setting for RAE should be changed from "All users" to "Only these users." The default setting "All users" includes all users on your local computer and all users in the directory server you are connected to.

When securely configuring RAE, restrict remote events to only be accepted from specific users. This prevents unauthorized users form sending malicious events to your computer. If you create a sharing user account, create a strong password using Password Assistant. Avoid accepting events from Mac OS 9 computers. If you need to accept Mac OS 9 events, use Password Assistant to create a strong password.

Securing Network and Host Access Services

15

Use this chapter to learn how to secure Network and Host Access services.

You can tailor network and host access services in Leopard Server to protect your computer and network users. Proper configuration of services is important and helps create a hardened shell protecting your network.

Leopard Server includes several network and host access services that help you manage and maintain your network. This section describes recommended configurations for securing your network services.

For additional information about configuring network and host access services, see the *Network Services Administration* guide.

Using IPv6 Protocol

Internet Protocol Version 6 (IPv6) is the Internet's next-generation protocol designed to replace the current Internet Protocol, IP Version 4 (IPv4, or just IP).

IPv6 improves routing and network autoconfiguration. It increases the number of network addresses to over 3 x10^{38}, and eliminates the need for Network Address Translation (NAT). IPv6 is expected to gradually replace IPv4 over a number of years, though the two will continue to coexist during this transition.

Leopard Server's network services are fully IPv6 capable and ready to transition to the next generation addressing as well as being fully able to operate with IPv4

Leopard Server fully supports IPv6, which is configurable from Network preferences. Disable the IPv6 protocol if your server and clients do not require it. Disabling the protocol prevents potential vulnerabilities on your computer. For information about disabling IPv6, see "Securing Network Preferences" on page 132.

To enable IPv6:

1. Open Network preferences.
2. In the network connections services list, click the service to configure.

3 Click Advanced.

4 Click TCP/IP.

5 Choose Automatically from the Configure IPv6 pop-up menu.

If you choose Manually, you will need to know your assigned IPv6 address, your router's IP address, and a prefix length.

6 Click OK.

7 Click Apply.

From the Command Line:

```
# ---------------------------------------------------------------------
# Enabling IPv6
# ---------------------------------------------------------------------

# Enable IPv6
# ------------------------------
networksetup -setv6on [networkservice]
```

IPv6-Enabled Services

The following services in Leopard Server support IPv6 addressing:

- DNS (BIND)
- Firewall
- Mail (POP/IMAP/SMTP)
- Windows (SMB/CIFS)
- Web (Apache 2)

These services support IPv6 addresses, but not in Server Admin. IPv6 addresses fail if entered in IP address fields in Server Admin. IPv6 addresses for these services can be configured with command-line tools and by editing configuration files.

A number of command-line tools installed with Leopard Server support IPv6 (for example, `ping6` and `traceroute6`).

For more information about IPv6, see www.ipv6.org.

Securing DHCP Service

Leopard Server includes dynamic host configuration protocol (DHCP) service software, which allows it to provide IP addresses, LDAP server information, and DNS server information to clients.

Disabling Unnecessary DHCP Services

Using DHCP is not recommended. Assigning static IP addresses eases accountability and mitigates the risks posed by a rogue DHCP server. If DHCP use is necessary, only one system should act as the DHCP server and the service should be disabled on all other systems.

To disable the DHCP service:

1. Open Server Admin and connect to the server.
2. Select the server name.
3. Click Settings.
4. Click Services.
5. Deselect DHCP.
6. Click Save.

From the Command Line:

```
# ---------------------------------------------------------------------
# Securing DHCP Service
# ---------------------------------------------------------------------

# Disable DHCP Service
# --------------------
serveradmin stop dhcp
```

Configuring DHCP Services

To use a server as a DHCP server, configure the DHCP service in Server Admin to *not* distribute DNS, LDAP, and WINS information. This is a security measure meant to protect client systems. When client systems accept dynamically assigned DNS, LDAP, and WINS addresses, they become vulnerable to certain forms of network based attacks from rogue DHCP servers. Users may unknowingly be redirected to malicious web sites or servers.

To configure the DHCP service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select DHCP, then select Subnets.
4. Select a subnet.
5. Click DNS.
6. Delete any name servers listed.

7 Click LDAP.

8 Delete any server information that appears.

9 Click WINS.

10 Delete the WINS information.

11 Click Save.

From the Command Line:

```
# Configuring DHCP Services
# -------------------------
# Set a DHCP subnet's DNS, LDAP, and WINS parameters to no value
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-
     AEE5-BED51A44775D:dhcp_domain_name_server:_array_index:0 = ""
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-
     AEE5-BED51A44775D:dhcp_ldap_url:_array_index:0 = -empty_array
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-
     AEE5-BED51A44775D:WINS_node_type =" NOT SET"
```

Assigning Static IP Addresses Using DHCP

You can use Server Admin to assign IP addresses to specific computers. This helps simplify configuration when using DHCP and lets you have some static servers or services.

To avoid potential address conflicts and prevent hackers from easily obtaining valid IP addresses, use a static map to track network activity. A static map consist of a specific IP address assigned to a network device.

To assign a static IP address to a device, you need the device's Ethernet address (sometimes called its MAC address or hardware address). Each network interface has its own Ethernet address.

If you have a computer that moves from being wired to the network to a wireless network, it uses two different Ethernet addresses, one for the wired connection, and one for the wireless connection.

To assign a static IP address:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select DHCP.

4 Click Static Maps.

5 Click Add Computer.

6 Enter the name of the computer.

7 In the Network Interfaces list, click the column to enter the following information:

MAC Address of the computer that needs a static address.

IP address you want to assign to the computer.

8 If your computer has other network interfaces that require static IP addresses, click the Add (+) button and enter the IP address you want to assign for each interface.

9 Click OK.

10 Click Save.

Securing DNS Service

Leopard Server uses Berkeley Internet Name Domain (BIND) v9.4.1 for its implementation of DNS protocols. BIND is an open source implementation and is used by most name servers on the Internet.

If your server is not intended to be a DNS server, disable the DNS service in Server Admin.

To disable the DNS service:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select the server name.

4 Click Settings.

5 Click Services.

6 Deselect DNS.

7 Click Save.

From the Command Line:

```
# ------------------------------------------------------------------------
# Securing DNS Service
# ------------------------------------------------------------------------

# Disable DNS Service
# -------------------
serveradmin stop dns
```

Understanding BIND

BIND is the set of programs used by Leopard Server that implements DNS. One of those programs is the *name daemon,* or *named*. To set up and configure BIND, you must change the configuration file and the zone file. The configuration file is /etc/named.conf.

The zone file name is based on the name of the zone. For example, the zone file example.com is /var/named/example.com.zone.

If you edit named.conf to configure BIND, don't change the `inet` settings of the controls statement. Otherwise, Server Admin can't retrieve status information for DNS.

The `inet` settings should look like this

```
controls {
       inet 127.0.0.1 port 54 allow {any;}
       keys { "rndc-key"; };
};
```

Using Server Admin after editing the BIND configuration files might overwrite some changes.

For more information about DNS and BIND, see the following:

- *DNS and BIND, 5th edition*, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 2006)
- The International Software Consortium website: www.isc.org and www.isc.org/sw/bind
- The DNS Resources Directory: www.dns.net/dnsrd

Turning Off Zone Transfers

Unless your site requires them, use Server Admin to turn off zone transfers and recursive DNS queries.

To turn off zone transfers and recursive DNS queries:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select DNS.
4. Click Zones.
5. Select the primary zone you want to change.
6. Click General.

7 Deselect "Allows zone transfer" to prevent hosts on the network from getting copies of the primary zone data.

If needed, zone transfers should be set up so they only occur between trusted servers. This requires manually editing the BIND configuration files.

8 Click Save.

Disabling Recursion

Recursion fully resolves domain names into IP addresses. Applications depend on the DNS server to perform this function. Other DNS servers that query your DNS servers don't need to perform the recursion.

To prevent malicious users from changing the primary zone's records (referred to as cache poisoning) and to prevent unauthorized use of the server for DNS service, you can restrict recursion using Server Admin. However, if you prevent your private network from using recursion, your users can't use your DNS service to look up names outside of your zones.

Disable recursion only if no clients are using this DNS server for name resolution and no servers are using it for forwarding.

If your site requires recursion, allow recursive queries only from trusted clients and not from external networks.

If you enable recursion, consider disabling it for external IP addresses but enabling it for internal IP addresses. This requires manually editing the BIND configuration files.

To disable recursion:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select DNS.

4 Click Settings.

5 Remove all entries from the "Accept recursive queries from the following networks" list using the Remove (–) button.

6 Click Save.

Make sure that both forward and reverse zones are established and fully populated. Otherwise, any Open Directory server using the DNS service will not work correctly.

Understanding DNS Security

DNS servers are targeted by malicious computer users (hackers). DNS servers are susceptible to several kinds of attacks. By taking extra precautions, you can prevent the problems and downtime associated with hackers.

Several kinds of security attacks are associated with DNS service:

- DNS cache poisoning
- Server mining
- DNS service profiling
- Denial of service (DoS)
- Service piggybacking

For more information about network attack patterns, refer to the relevant external sources on the subject.

DNS Cache Poisoning

DNS cache poisoning (a form of DNS spoofing) is the adding of false data to the DNS server's cache. This enables hackers to:

- Redirect real domain name queries to alternative IP addresses.

 For example, a falsified A record for a bank could point a computer user's browser to a different IP address that is controlled by the hacker. A duplicate website could fool users into giving their bank account numbers and passwords to the hacker.

 Also, a falsified mail record could enable a hacker to intercept mail sent to or from a domain. If the hacker then forwards that mail to the correct mail server after copying the mail, this can go undetected.

- Prevent proper domain name resolution and access to the Internet.

 This is the most benign of DNS cache poisoning attacks. It makes a DNS server appear to be malfunctioning.

The most effective method to prevent these attacks is vigilance. This includes maintaining up-to-date software.

If exploits are found in the current version of BIND, the exploits are patched and a security update is made available for Leopard Server. Apply all such security patches.

Server Mining

Server mining is the practice of getting a copy of a complete primary zone by requesting a zone transfer. In this case, a hacker pretends to be a secondary zone to another primary zone and requests a copy of the primary zone's records.

With a copy of your primary zone, the hacker can see what kinds of services a domain offers and the IP addresses of the servers that offer them. He or she can then try specific attacks based on those services. This is reconnaissance before another attack.

To prevent this attack, disable zone transfers. If required, specify which IP addresses have permission to request zone transfers (your secondary zone servers) and deny all others.

Zone transfers are accomplished over TCP on port 53. To limit zone transfers, block zone transfer requests from anyone but your secondary DNS servers.

To specify zone transfer IP addresses:

1. Create a firewall filter that permits only IP addresses that are inside your firewall to access TCP port 53.
2. Follow the instructions in "Creating Advanced Firewall Rules" on page 234 using the following settings:
 - Packet: Allow
 - Port: 53
 - Protocol: TCP
 - Source IP: the IP address of your secondary DNS server
 - Destination IP: the IP address of your primary DNS server

DNS Service Profiling

Another common reconnaissance technique used by malicious users is to profile your DNS service. First a hacker makes a BIND version request. The server reports what version of BIND is running. The hacker then compares the response to known exploits and vulnerabilities for that version of BIND.

To prevent this attack, configure BIND to respond with something other than what it is.

To alter BIND's version response:

1. Open a command-line text editor (for example `vi`, `emacs`, or `pico`).
2. Open named.conf for editing.
3. To the options brackets of the configuration file, add the following:

```
version    "[your text, maybe 'we're not telling!']";
```

4. Save named.conf.

Denial of Service (DoS)

This kind of attack is common and easy. A hacker sends so many service requests and queries that a server uses all its processing power and network bandwidth trying to respond. The hacker prevents legitimate use of the service by overloading it.

It is difficult to prevent this type of attack before it begins. Constant monitoring of the DNS service and server load enables an administrator to catch the attack early and mitigate its damaging effect.

The easiest way to prevent this attack is to block the offending IP address with your firewall. Unfortunately, this means the attack is already underway and the hacker's queries are being answered and the activity logged.

Service Piggybacking

This attack is done not so much by malicious intruders but by common Internet users who learn the trick from other users. They might feel that the DNS response time with their own ISP is too slow, so they configure their computer to query another DNS server instead of their own ISP's DNS servers. Effectively, there are more users accessing the DNS server than were planned for.

You can prevent this type of attack by limiting or disabling DNS recursion. If you plan to offer DNS service to your LAN users, they need recursion to resolve domain names, but don't provide this service to Internet users.

To prevent recursion entirely, see "Disabling Recursion" on page 227.

The most common balance is permitting recursion for requests coming from IP addresses in your own range but denying recursion to external addresses.

BIND enables you to specify this in its configuration file, named.conf. Edit your named.conf file to include the following:

```
options {
…
  allow-recursion{
     127.0.0.0/8;
     [your internal IP range of addresses, like 192.168.1.0/27];
               };
     };
```

For more information, see the BIND documentation.

ARP Spoofing

This type of attack, also known as ARP poisoning, allows an attacker to take over a computer's IP address by manipulating the ARP caches of other hosts on the network. The attacker must be on the same network as the computer it is attacking or the host that the computer is communicating with.

The attacker can also use ARP spoofing for a man-in-the-middle attack, which forwards traffic from a computer to the attacker's computer. This allows the attacker to view packets and look for passwords and confidential data. ARP spoofing can also be used to create a DoS attack, stopping all network traffic.

By configuring your network with static IP addresses and monitoring your network traffic, you can keep unauthorized users from maliciously using your network.

Securing Firewall Service

Firewall service is software that protects network applications running on your Leopard Server computer.

Turning on Firewall service is similar to installing a filter to limit access to your network. Firewall service scans incoming IP packets and rejects or accepts these packets based on rules you use to configure Firewall service.

You can restrict access to any IP service running on the server, and you can customize rules for incoming clients or for a range of client IP addresses.

Important: Firewall service can disrupt network communications and its configuration can be complicated to implement. Do not implement recommendations without understanding their purpose or impact.

Services such as Web and FTP services are identified on your server by a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number. When a computer tries to connect to a service, Firewall service scans the rule list for a matching port number.

The default firewall configuration on Leopard Server denies access to incoming packets from remote computers except through ports for remote configuration. This provides a high level of security.

Stateful rules are in place as well, so responses to outgoing queries initiated by your computer are also permitted. You can then add IP rules to permit server access to those clients who require access to services.

Important: You should not perform any server configuration remotely—particularly Firewall service, because of the risk of disabling communications to the remote host.

Planning Firewall Setup

Plan your Firewall service by deciding which services you want to provide access to. Mail, Web, and FTP services generally require access by computers on the Internet. File and Print services are most likely restricted to your local subnet.

After you decide which services to protect using Firewall service, you must determine which IP addresses you want to allow access to your server and which IP addresses you want to deny access to your server. You can then create the appropriate rules.

After the Firewall service is configured, network users might request that the rules be changed to allow additional services. These changes should be resisted and an approval process should be put in place to monitor these changes.

Advanced configuration servers use ipfw2 for firewall service. The application-level firewall is available only to standard and workgroup configuration installations.

Starting Firewall Service

By default, Firewall service blocks incoming TCP connections and denies UDP packets, except those received in response to outgoing requests from the server.

Before you turn on Firewall service, make sure you've set up rules permitting access from IP addresses you choose; otherwise, no one can access your server.

If you add or change a rule after starting Firewall service, the new rule affects connections already established with the server. For example, if you deny all access to your FTP server after starting Firewall service, computers connected to your FTP server are disconnected.

To start Firewall service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click the Start Firewall button below the Servers list.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Firewall Service
# ------------------------------------------------------------------

# Start Firewall service
# ----------------------
serveradmin start ipfilter
```

Creating an IP Address Group

By grouping IP addresses you can simultaneously set firewall rules for large numbers of network devices and allow for much better organization. This enhances the security if your network.

These groups are used to organize and target the rules. The "any" address group is for all addresses. Two other IP address groups are present by default, intended for the entire "10.0.0.0" range of private addresses and the entire "192.168.0.0" range of private addresses.

Addresses can be listed as individual addresses (192.168.2.2), IP address and CIDR notation (192.168.2.0/24), or IP address and netmask notation (192.168.2.0:255.255.255.0).

By default, an IP address group is created for all incoming IP addresses. Rules applied to this group affect all incoming network traffic.

To create an address group:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Settings, then click Address Groups.
5. Below the IP Address Groups list, click the Add (+) button.
6. In the Group name field, enter a group name.
7. Enter the addresses and subnet mask you want the rules to affect.

 Use the Add (+) and Delete (–) buttons.

 To indicate any IP address, use the word "any."
8. Click OK.
9. Click Save.

Creating Firewall Service Rules

By default, Firewall service permits all UDP connections and blocks incoming TCP connections on ports that are not essential for remote administration of the server. Also, by default, stateful rules are in place that permit specific responses to outgoing requests.

Before you turn on Firewall service, make sure you've set up rules permitting access from IP addresses you choose; otherwise, no one can access your server.

You can easily permit standard services through the firewall without advanced and extensive configuration. Standard services include:

- SSH access
- Web service
- Apple File service
- Windows File service
- FTP service
- Printer Sharing
- DNS/Multicast DNS
- ICMP Echo Reply (incoming pings)
- IGMP
- PPTP VPN
- L2TP VPN
- QTSS media streaming
- iTunes Music Sharing

If you add or change a rule after starting Firewall service, the new rule affects connections already established with the server. For example, if you deny all access to your FTP server after starting Firewall service, computers connected to your FTP server are disconnected.

To configure firewall standard services:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Settings, then click Services.
5. From the Edit Services for pop-up menu, select an address group.
6. For the address group, choose to permit all traffic from any port or to permit traffic on designated ports.
7. For each service you want the address group to use, select Allow.

 If you don't see the service you need, add a port and description to the services list.

 To create a custom rule, see "Creating Advanced Firewall Rules" on page 234.
8. Click Save.

Creating Advanced Firewall Rules

You use the Advanced Settings pane in Server Admin to configure specific rules for Firewall service. Firewall rules contain originating and destination IP addresses with subnet masks. They also specify what to do with incoming network traffic. You can apply a rule to all IP addresses, a specific IP address, or a range of IP addresses.

Addresses can be listed as individual addresses (192.168.2.2), IP address and subnet mask in CIDR notation (192.168.2.0/24), or IP address and subnet mask in netmask notation (192.168.2.0:255.255.255.0).

To set up an advanced firewall rule:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Settings, then click Advanced.
5. Click the Add (+) button.

 Alternatively, you can select a rule similar to the one you want to create, click Duplicate, and then click Edit.

6. In the Action pop-up menu, select whether this rule permits or denies access.

 If you choose Other, enter the needed action (for example, log).

7. From the Protocol pop-up menu, choose a protocol.

 If you choose Other, enter the needed protocol (for example, icmp, esp, ipencap).

8. From the Service pop-up menu, choose a service.

 To select a nonstandard service port, choose Other.

9. If needed, choose to log all packets that match the rule.

10. For the source of filtered traffic, choose an address group from the Address pop-up menu.

 If you don't want to use an existing address group, enter the source IP address range (using CIDR notation) you want to filter.

 If you want it to apply to any address, choose "any" from the pop-up menu.

11. If you selected a nonstandard service port, enter the source port number.

12. For the destination of filtered traffic, choose an address group from the Source pop-up menu.

 If you don't want to use an existing address group, enter the destination IP address range (using CIDR notation).

 If you want it to apply to any address, choose "any" from the pop-up menu.

13. If you selected a nonstandard service port, enter the destination port number.

14. From the Interface pop-up menu that this rule will apply to, choose In or Out.

 In refers to the packets being sent to the server.

 Out refers to the packets being sent from the server.

15. If you select Other, enter the interface name (en0, en1, fw1, and so on).

16. Click OK.

17. Click Save to apply the rule immediately.

Enabling Stealth Mode

You can hide your firewall by choosing not to send a connection failure notification to any connection that is blocked by the firewall. This is called stealth mode and it effectively hides your server's closed ports.

For example, if a network intruder tries to connect to your server, even if the port is blocked, he or she knows that there is a server and can find other ways to intrude.

If stealth mode is enabled, instead of being rejected, the hacker won't receive notification that an attempted connection took place.

To enable stealth mode:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Settings, then click Advanced.
5. Select "Enable for TCP," "Enable for UDP," or both, as needed.
6. Click Save.

From the Command Line:

```
# Enable stealth mode
# -------------------
serveradmin settings ipfilter:blackHoleTCP = true
serveradmin settings ipfilter:blackHoleUDP = true
```

Viewing the Firewall Service Log

Each rule you set up in Server Admin corresponds to rules in the underlying firewall software. Log entries show you when the rule was applied, the IP address of the client and server, and other information.

The log view shows the contents of /var/log/ipfw.log. You can refine the view using the text filter box.

To view the Firewall service log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Log.

 To search for specific entries, use the Filter field above the log.

From the Command Line:

```
# View the Firewall service log
# -----------------------------
tail /var/log/ipfw.log
```

The filters you create in Server Admin correspond to rules in the underlying filtering software. Log entries show you the rule applied, the IP address of the client and server, and other information. For more information about rules and what they mean, see "Creating Advanced Firewall Rules" on page 234.

Here are some examples of firewall log entries and how to read them.

Log Example 1

```
Dec 12 13:08:16 ballch5 mach_kernel: ipfw: 65000 Unreach TCP
     10.221.41.33:2190 192.168.12.12:80 in via en0
```

This entry shows that Firewall service used rule 65000 to deny (unreach) the remote client at 10.221.41.33:2190 from accessing server 192.168.12.12 on web port 80 through Ethernet port 0.

Log Example 2

```
Dec 12 13:20:15 mayalu6 mach_kernel: ipfw: 100 Accept TCP 10.221.41.33:721
     192.168.12.12:515 in via en0
```

This entry shows that Firewall service used rule 100 to permit the remote client at 10.221.41.33:721 to access the server 192.168.12.12 on the LPR printing port 515 through Ethernet port 0.

Log Example 3

```
Dec 12 13:33:15 smithy2 mach_kernel: ipfw: 10 Accept TCP 192.168.12.12:49152
     192.168.12.12:660 out via lo0
```

This entry shows the NAT divert rule applied to an outbound packet. In this case it diverts the rule to service port 660, which is the port the NAT daemon uses.

Securing NAT Service

NAT is a protocol you use to give multiple computers access to the Internet using only one assigned public or external IP address. NAT permits you to create a private network that accesses the Internet through a NAT router or gateway. NAT is sometimes referred to as IP masquerading.

The NAT service further enhances security by limiting communication between your private network and a public network (such as the Internet):

- Communication from a computer on your private network is translated from a private IP address to a shared public IP address. Multiple private IP addresses are configured to use a single public IP address.
- Communication to your private network is translated and forwarded to an internal private IP address (IP forwarding). The external computer cannot determine the private IP address. This creates a barrier between your private network and the public network.

- Communication from a public network cannot come into your private network unless it is requested. It is only allowed in response to internal communication.

Note: If using NAT, consider combining NAT routing with other network services.

The NAT router takes all traffic from your private network and remembers internal addresses that have made requests. When the NAT router receives a response to a request, it forwards it to the originating computer. Traffic that originates from the Internet does not reach computers behind the NAT router unless port forwarding is enabled.

Important: Firewall service must be enabled for NAT to function.

If your server is not intended to be a NAT server, deactivate the NAT server software.

To disable NAT service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect NAT.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing NAT Service
# ------------------------------------------------------------------

# Disable NAT service
# -------------------
serveradmin stop nat
```

Configuring NAT Service

Use Server Admin to indicate which network interface is connected to the Internet or other external network.

To configure NAT service:

1. In Server Admin, select NAT in the Computers & Services list.
2. Click Settings.
3. Select "IP Forwarding and Network Address Translation."

4 From the "Network connection to share" pop-up menu choose the network interface.

This interface should be the one that connects to the Internet or external network.

5 Click Save.

Configuring Port Forwarding

You can direct traffic coming in to your NAT network to a specific IP address behind the NAT gateway. This is called *port forwarding*.

Port forwarding lets you set up computers on the internal network that handle incoming connections without exposing other computers to outside connections. For example, you could set up a web server behind the NAT service and forward incoming TCP connection requests on port 80 to the designated web server.

You can't forward the same port to multiple computers, but you can forward many ports to one computer. Enabling port forwarding requires the use of the Terminal application and administrator access to root privileges through `sudo`.

You must also create a plist file. The contents of the plist file are used to generate /etc/nat/natd.conf.apple, which is passed to the NAT daemon when it is started.

Do not try to edit /etc/nat/natd.conf.apple directly. If you use a plist editor instead of a command-line text editor, alter the following procedure to suit.

To configure port forwarding:

1 If the file /etc/nat/natd.plist doesn't exist, make a copy of the default NAT daemon plist.

```
$ sudo cp /etc/nat/natd.plist.default /etc/nat/natd.plist
```

2 Using a Terminal editor, add the following block of XML text to /etc/nat/natd.plist before the two lines at the end of the file (</dict> and </plist>), substituting your settings where indicated by italics:

```
<key>redirect_port</key>
  <array>
     <dict>
          <key>proto</key>
          <string>tcp or udp</string>
          <key>targetIP</key>
          <string>LAN_ip</string>
          <key>targetPortRange</key>
          <string>LAN_ip_range</string>
          <key>aliasIP</key>
          <string>WAN_ip</string>
          <key>aliasPortRange</key>
          <string>WAN_port_range</string>
     </dict>
  </array>
```

3 Save your file changes.

4 Enter the following commands in the Terminal:

```
$ sudo systemstarter stop nat
$ sudo systemstarter start nat
```

5 Verify that your changes remain by inspecting the /etc/nat/natd.conf.apple file.

The changes made, except for comments and those settings that Server Admin can change, are used by server configuration tools (Server Admin, Gateway Setup Assistant, and serveradmin).

6 Configure NAT service in Server Admin as needed.

For more information, see "Configuring NAT Service" on page 238.

7 Click Save.

8 Start NAT service.

Securing Bonjour Service

With Bonjour, you can share nearly anything, including files, media, printers, and other devices, in innovative and easier ways. It simplifies traditional network-based activities like file sharing and printing by providing dynamic discoverability of file servers and Bonjour-enabled network printers.

Users and applications on your local network can use Bonjour to quickly determine which services are available on your computer, and you can use Bonjour to discover what services are offered by other systems on the network. Any network service incurs a security risk, and if it is not necessary, it should be disabled.

If Bonjour is necessary, its usage can be restricted by DNS clients.

To disable DNS service Bonjour settings:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select DNS.

4 Click Bonjour.

5 To disable wide-area Bonjour browsing, deselect "Enable automatic client Bonjour browsing for domain."

6 Click Save.

You won't be able to use network printing using Bonjour, so you'll need to manually configure network printers. This can also disable some functionality in other applications that rely on Bonjour, or possibly make them unusable. For example, there are issues with calendar and address book sharing, and finding iChat buddies.

If disabling Bonjour causes vital applications to break, enable it. If you decide to reenable Bonjour, block UDP port 5353 on your firewall to block externally originating Bonjour traffic.

Securing Collaboration Services 16

Use this chapter to learn how to secure collaboration services.

Collaboration services help users share information for increased productivity. Securing the access and transfer of shared information protects your data.

Collaboration services promote interactions among users, facilitating teamwork and productivity. This chapter describes how to secure iCal, iChat, Wiki, and Podcast Producer collaboration services.

For information about configuring collaboration services, see *iCal Service Administration*, *iChat Service Administration*, *Web Technologies Administration*, and *Podcast Producer Administration*.

Securing iCal Service

Security for iCal service consists of two main areas:

- **Securing the authentication:** This means using a method of authenticating users that is secure and doesn't pass the login credentials in clear text over the network. The high-security authentication used pervasively in Leopard Server is Kerberos v5.

 To learn how to configure secure authentication, see "Choosing and Enabling Secure Authentication for iCal Service" on page 243.

- **Securing the data transport:** This means encrypting the network traffic between the calendar client and the calendar server. When the transport is encrypted, no one can analyze the network traffic and reconstruct the contents of the calendar. iCal service uses SSL to encrypt the data transport.

 To learn how to configure and enable SSL for iCal service, see "Configuring and Enabling Secure Network Traffic for iCal Service" on page 244.

Disabling iCal Services

If your server is not intended to be an iCal server, disable the iCal server software. Disabling the service prevents potential vulnerabilities on your computer.

To disable iCal service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click iCal.
4. Click Stop iCal (below the Servers list).

From the Command Line:

```
# ---------------------------------------------------------------------
# Securing iCal Service
# ---------------------------------------------------------------------

# disable iCal service
# ------------------------------
serveradmin stop calendar
```

Securely Configuring iCal Service

To securely configure iCal service, you must secure authentication and data transport.

Choosing and Enabling Secure Authentication for iCal Service

Users authenticate to iCal service through one of the following methods:

- **Kerberos v5:** This method uses strong encryption and is used in Leopard for single sign-on to services offered by Leopard Server.
- **Digest:** (RFC 2617) This method sends secure login names and encrypted passwords without the use of a trusted third-party (like the Kerberos realm), and is usable without maintaining a Kerberos infrastructure.
- **Any:** This method includes Kerberos v5 and Digest authentication. The client can choose the most appropriate method for what it can support.

You can set the required authentication method using Server Admin. To enable the highest security, choose a method other than "Any."

To choose an authentication method:

1. In Server Admin, select a server and choose the iCal service.
2. Click the Settings button in the toolbar.
3. Select the method from the Authentication pop-up menu.
4. Click Save, then restart the service.

From the Command Line:

```
# Choose an authentication method for iCal service
# To enable all auth methods:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar

# To choose Digest auth only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "no"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar

# For Kerberos only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "no"
serveradmin stop calendar; sudo serveradmin start calendar
```

Configuring and Enabling Secure Network Traffic for iCal Service

When you enable Secure Sockets Layer (SSL), you encrypt all data sent between the iCal server and the client. To enable SSL, you must select a certificate. If you use the default self-signed certificate, the clients must choose to trust the certificate before they can make a secure connection.

To enable secure network traffic using SSL transport:

1. In Server Admin, select a server and choose the iCal service.
2. Click the Settings button in the toolbar.
3. Click Enable Secure Sockets Layer (SSL).
4. Choose a TCP port for SSL to communicate on.

 The default port is 8443.
5. Choose the certificate to be used for encryption.
6. Click Save, then restart the service.

From the Command Line:

```
# Enable secure network traffic using SSL transport
serveradmin settings calendar:SSLPort = 8443
```

Viewing iCal Service Logs

iCal service logging is important for security. With logs, you can monitor and track communication through the iCal service. The iCal service log, /var/log/system.log, can be accessed using Server Admin.

To view the iCal service log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click iCal.
4. Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the iCal service log
tail /var/log/caldavd/access.log
```

Securing iChat Service

The iChat service provides a secure way for users to chat. To use iChat service on a server, users must be defined in directories the server uses to authenticate users. For more information about configuring search paths to directories, see the *Open Directory Administration* guide.

Disabling iChat Service

If your server is not intended to be an iChat server, disable the iChat server software. Disabling the service prevents potential vulnerabilities on your computer.

To disable iChat service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click iChat.
4. Click Stop iChat (below the Servers list).

From the Command Line:

```
# Disable iChat service
serveradmin stop jabber
```

Securely Configuring iChat Service

If your organization requires the use of iChat service, configure it to use SSL. SSL communication certifies the identity of the server and establishes secure, encrypted data exchange.

You identify an SSL certificate for iChat service to use the first time you set up iChat service, but you can use a different certificate later if you like. You can use a self-signed certificate or a certificate imported from a Certificate Authority. For more information about defining, obtaining, and installing certificates on your server, see "Obtaining Certificates" on page 191.

Sending messages to multiple recipients over an internal iChat sever does not require a MobileMe identity. The internal iChat server (Jabberd) requires a server-side SSL certificate that is used by each client to establish an SSL session (similar to a web access session). A MobileMe certificate is required to establish encrypted sessions between two iChat clients communicating using text, audio, and video.

To securely configure iChat service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select iChat.
4. Click Settings, then click General.
5. Click the Add (+) button to add host domains.

 The Host Domains list designates the domain names you want iChat to support. Initially, the server host name is shown. You can add or remove other names that resolve to the iChat service IP address such as aliases defined in DNS. When starting iChat, you must specify a DNS for the service.

 Host domains are used to construct Jabber IDs, which identify iChat users. An example of a Jabber ID is nancy@example1.apple.com.
6. From the SSL Certificate pop-up menu, choose an SSL certificate.

 The menu lists all SSL certificates that have been installed on the server.

 To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.

 For more information about increasing server security, see *Mac OS X Server Security Configuration*. Information about creating and managing server certificates can also be found in *Server Administration*.
7. Choose the method of authentication from the Authentication pop-up menu:

 Choose Standard if you want iChat to only accept password authentication.

 Choose Kerberos if you want iChat to only accept Kerberos authentication.

 Choose Any Method if you want iChat to accept password and Kerberos authentication.
8. To permit iChat to communicate with other XMPP-compliant chat servers, select "Enable XMPP server-to-server federation."

9 If you are using a certificate with iChat, select "Require secure server-to-server federation."

This option requires an SSL certificate to be installed, which is used to secure the server-to-server federation.

10 To restrict server-to-server communication to servers that are listed, select "Allow federation with the following domains."

You can add or remove domains using the Add (+) or Delete (–) buttons below the list.

11 Click Save, and then click Start Service.

12 Make sure the iChat server's Open Directory search path includes directories in which the users and group members that you want to communicate using iChat service are defined.

The *Open Directory Administration* guide explains how to set up search paths.

Any user or group member defined in the Open Directory search path is now authorized to use iChat service on the server, unless you deny them access to iChat service.

From the Command Line:

```
# Securely configure iChat service
# To select an iChat server certificate:
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"

# (Or replace the path with the full path to the certificate that you want
# to select.)
# Restart the service if it is running
serveradmin stop jabber; sudo serveradmin start jabber

# To select an iChat server auth method you would use one of the following:
serveradmin settings jabber:authLevel = "ANYMETHOD"
serveradmin settings jabber:authLevel = "KERBEROS"
serveradmin settings jabber:authLevel = "STANDARD"

# Then restart the service:
serveradmin stop jabber
serveradmin start jabber
```

Using Certificates to Secure S2S Communication

Using Server Admin, you can secure S2S communication with certificates.

By default, iChat selects a port using a preinstalled, self-signed SSL certificate. You can select your own certificate. The selected certificate is used for client-to-server communications on ports 5222 and 5223 and for server-to-server communications.

Jabber provides the following ports:

- 5222 accepts TLS encryption
- 5223 accepts SSL encryption

SSL encrypts your chat message over the network between client-to-server and server-to-server connections. However, if your iChat server is logging chat messages, your messages are stored in a unencrypted format that can be easily viewed by your server administrator.

To select a certificate:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select iChat.
4. Click Settings, then click General.
5. From the SSL Certificate pop-up menu, choose an SSL certificate.

 The menu lists all SSL certificates that are installed on the server.

 To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.

 For more information about creating and managing server certificates, see *Server Administration*.
6. Click Save.

From the Command Line:

```
# Select a certificate
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"
```

Additional Security Enhancements

For additional security enhancements, you can further restrict the iChat service by using SACLs and firewall rules. These are configured based on your organizations network environment.

You can configure SACLs to restrict iChat access to specific users or groups. For more information about configuring SACLs, see "Setting Service Access Control Lists" on page 205.

You can configure firewall rules that prevent iChat connections from unintended sources. For more information, see "Creating Firewall Service Rules" on page 233.

Viewing iChat Service Logs

iChat service logging is important for security. With logs, you can monitor and track communication through the iChat service. Access the iChat service log, /var/log/system.log, using Server Admin.

To view the iChat service log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click iChat.
4. Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the iChat service log
tail /var/log/server.log | grep jabberd
```

Securing Wiki Service

The level of website security determines the level of wiki security. Wiki security is established when the website that the wiki is configured on is secure.

Disabling Web Service

If your server is not intended to provide Wiki services, disable the Web server software. Disabling Web service prevents potential vulnerabilities on your computer.

To disable Web service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click Web.
4. Click Stop Web (below the Servers list).

From the Command Line:

```
# ------------------------------------------------------------------------
# Securing Wiki Service
# ------------------------------------------------------------------------

# Disable Web service
serveradmin stop teams
```

Securely Configuring Wiki Services

Methods you can use to help secure data moving to and from your wiki include the following:

- Set up SSL for the website your wiki is running on. SSL provides security for a site and its users by authenticating the server, encrypting information, and maintaining message integrity. For more information, see "Enabling Secure Sockets Layer (SSL)" on page 290.
- Restrict users and groups that can create wiki pages on your website by adding users and groups to the Web services list. For more information, see "Securing Web Service" on page 285.

Viewing Wiki Service Logs

Wiki service logging is important for security. With logs, you can monitor and track communication through the Wiki service. Access the Wiki service logs, /Library/Logs/wikid/error.log and /Library/Logs/wikid/access.log, using Server Admin.

To view the Wiki service log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click Wiki.
4. Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the Wiki service log
tail /Library/Logs/wikid/access.log
```

Securing Podcast Producer Service

To secure Podcast Producer service, disable it if you don't use it. If you use the service, use Server Admin to control access to workflows and cameras.

Disabling Podcast Producer Service

If your server is not intended to be a Podcast Producer server, disable the Podcast Producer server software. Disabling the service prevents potential vulnerabilities on your computer.

To disable Podcast Producer service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click Podcast Producer.
4. Click Stop Podcast Producer (below the Servers list).

From the Command Line:

```
# Disable Podcast Producer service
serveradmin stop pcast
```

Securely Configuring Podcast Producer Service

To protect the Podcast Producer service from being exploited, control access to workflows and cameras using Server Admin.

To control access to a workflow:

1. Open Server Admin.
2. In the Computers and Services list, select Podcast Producer.
3. Click Workflows.
4. Select a workflow in the Workflow list.
5. To restrict access to the workflow, click "Allow access to *workflow name* for the following users and groups."
6. Click the (+) button to add users and groups to the list of users and groups that can access the selected workflow.

 In the Users and Groups window, click Users and drag one or more users to the list.

 In the Users and Groups window, click Groups and drag one or more groups to the list.

 To delete users and groups from the list, select them and click (-).
7. Click Save.

To control access to a camera:

1. Open Server Admin.
2. In the Computers and Services list, select Podcast Producer.
3. Click Cameras.

4 Select a camera in the Cameras list.

5 To restrict access to the camera, click "Allow access to *camera name* for the following users and groups."

6 Click the (+) button to add users and groups to the list of users and groups that can access the selected camera.

In the Users and Groups window, click Users and drag users to the list.

In the Users and Groups window, click Groups and drag groups to the list.

To delete users or groups from the list, select them and click (-).

7 Click Save.

Viewing Podcast Producer Service Logs

Podcast Producer service logging is important for security. With logs, you can monitor and track communication through the Podcast Producer service. Access the Podcast Producer service log, /Library/Logs/pcastserverd/application.log, using Server Admin.

To view the Podcast Producer service log:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click Podcast Producer.

4 Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the Podcast Producer service log
tail /Library/Logs/pcastserverd/pcastserverd_out.log
```

Securing Mail Service

17

Use this chapter to learn how to secure Mail service.

Mail service is crucial in today's dispersed work environments. Protect your mail by using encryption, adaptive junk mail filtering, and virus detection.

Mail service in Leopard Server allows network users to send and receive mail over your network or across the Internet.

Mail service sends and receives mail using the following standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP).

Mail service also uses a Domain Name System (DNS) service to determine the destination IP address of outgoing mail.

Leopard Server uses Cyrus to provide POP and IMAP service. More information about Cyrus can be found at: asg.web.cmu.edu/cyrus.

Leopard Server uses Postfix as its mail transfer agent (MTA). Postfix fully supports SMTP. Your mail users will set their mail application's outgoing mail server to your Leopard Server running Postfix, and access incoming mail from a Leopard Server running incoming mail service. More information about Postfix can be found at: www.postfix.org.

For more information about configuring mail service, see the *Mail Service Administration* guide.

Disabling Mail Service

If your server is not intended to be a mail server, disable the mail service software. Disabling the service prevents potential vulnerabilities on your server. To disable Mail service, turn off support for the IMAP, SMTP, and POP protocols that are not required. Mail service is enabled by default (except in Advanced mode), so verification is recommended.

To disable Mail service protocols:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Make sure at least one protocol (SMTP, POP, or IMAP) is enabled.
5. Click Stop Service in the menu bar.

 When the service is turned on, the Stop Service button is available.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Mail Service
# ------------------------------------------------------------------

# Disable Mail service protocols
serveradmin settings mail:imap:enable_pop = no
serveradmin settings mail:imap:enable_imap = no
serveradmin settings mail:postfix:enable_smtp = no
```

Configuring Mail Service for SSL

If Mail service protocols are required, protect their communications using Secure Sockets Layer (SSL). SSL connections ensure that the data sent between your mail server and your users' mail clients is encrypted. This allows secure and confidential transport of mail messages across a local network.

SSL transport doesn't provide secure authentication. It provides secure transfer from your mail server to your clients. For secure authentication information, see *Open Directory Administration*.

For incoming mail, Mail service supports secure mail connections with mail client software that requests them. If a mail client requests an SSL connection, Mail service can comply if that option is enabled. Mail service still provides non-SSL (unencrypted) connections to clients that don't request SSL. The configuration of each mail client determines whether it connects with SSL or not.

For outgoing mail, Mail service supports secure mail connections between SMTP servers. If an SMTP server requests an SSL connection, Mail service can comply if that option is enabled. Mail service can still allow non-SSL (unencrypted) connections to mail servers that don't request SSL.

Enabling Secure Mail Transport with SSL

Mail service requires some configuration to provide SSL connections automatically. The basic steps are as follows:

Step 1: Obtain a security certificate

This can be done in the following ways:

- Get a certificate from a Certificate Authority (CA).
- Generate a Certificate Signing Request (CSR) and create a keychain.
- Use the CSR to obtain a certificate from an issuing CA or create a self-signed certificate in Server Admin's Certificate Manager.
- Locate an existing certificate from a previous installation of Mac OS X Server v10.3 or later.

 If you have already generated a security certificate in a previous version of Mac OS X Server, you can import it for use.

Step 2: Import the certificate into Server Admin's Certificate Manager

You can use Certificate Manager to drag and drop certificate information or you can provide Certificate Manager with the path to an existing installed certificate.

Step 3: Configure the service to use the certificate

For instructions for allowing or requiring SSL transport, see the following sections:

- "Configuring SSL Transport for POP Connections" on page 256
- "Configuring SSL Transport for IMAP Connections" on page 257
- "Configuring SSL Transport for SMTP Connections" on page 259

Enabling Secure POP Authentication

Your POP mail service can protect user passwords by allowing Authenticated POP (APOP) or Kerberos. When a user connects with APOP or Kerberos, the user's mail client software encrypts the user's password before sending it to your POP service. Before configuring Mail service to require secure authentication, make sure that users' mail applications and user accounts support the method of authentication you choose.

Before enabling Kerberos authentication for incoming mail service, you must integrate Leopard with a Kerberos server. If you're using Leopard Server for Kerberos authentication, this is already done for you. For more information, see *Open Directory Administration*.

If you want to *require* either of these authentication methods, enable only one method.

To set the POP authentication method:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.

4 Select Security.

5 Click the APOP or Kerberos checkbox in the POP3 list.

6 Click Save.

From the Command Line:

```
# Set the POP authentication method
serveradmin settings mail:imap:pop_auth_apop = no
serveradmin settings mail:imap:pop_auth_clear = no
serveradmin settings mail:imap:pop_auth_gssapi = no
```

Configuring SSL Transport for POP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for POP (and IMAP) connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for POP also sets it for IMAP.

To set SSL transport for POP connections:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Advanced tab.

4 Select Security.

5 In the IMAP and POP SSL pop-up menus, select Require or Use to enable (or Don't Use to disable).

6 Select the certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.

7 Click Save.

From the Command Line:

```
# Set SSL transport for POP connections
serveradmin settings mail:imap:tls_server_options = "use"
```

Enabling Secure IMAP Authentication

Your IMAP mail service can protect user passwords by requiring that connections use a secure method of authentication. You can choose CRAM-MD5 or Kerberos v5 authentication.

When a user connects with secure authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Make sure that your users' mail applications and user accounts support the method of authentication you choose.

If you configure Mail service to require CRAM-MD5, you must set mail accounts to use a Leopard Server Password Server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Leopard with a Kerberos server. If you're using Leopard Server for Kerberos authentication, this is done for you. For instructions, see *Open Directory Administration*.

If you want to *require* any of these authentication methods, enable only one method.

To set secure IMAP authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Select CRAM MD-5 or Kerberos (as needed) in the IMAP section.
6. Click Save.

From the Command Line:

```
# Set secure IMAP authentication
serveradmin settings mail:imap:imap_auth_login = no
serveradmin settings mail:imap:imap_auth_plain = no
serveradmin settings mail:imap:imap_auth_gssapi = no
serveradmin settings mail:imap:imap_auth_clear = no
serveradmin settings mail:imap:imap_auth_cram_md5 = no
```

Configuring SSL Transport for IMAP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for IMAP also sets it for POP.

To configure SSL transport for IMAP connections:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.

4 Select Security.

5 From the pop-up menus in the IMAP and POP SSL section click Require or Use to enable (Don't Use to disable).

6 Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.

7 Click Save.

From the Command Line:

```
# Configure SSL transport for IMAP connections (same as POP)
serveradmin settings mail:imap:tls_server_options = "use"
```

Enabling Secure SMTP Authentication

Your server can guard against being an open relay by allowing SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) You can configure Mail service to require secure authentication using CRAM-MD5 or Kerberos. You can also allow the less secure plain and login authentication methods, which don't encrypt passwords, if some users have mail client software that doesn't support secure methods.

If you configure Mail service to require CRAM-MD5, mail users' accounts must be set to use a password server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Leopard with a Kerberos server. If you're using Leopard Server for Kerberos authentication, this is done for you. For instructions, see *Open Directory Administration*.

Enabling SMTP Authentication will:

- Make your users authenticate with their mail client before accepting mail to send.
- Frustrate mail server abusers trying to send mail without your consent through your system.

If you want to *require* any of these authentication methods, enable only one method.

To allow secure SMTP authentication:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Advanced tab.

4 Select Security.

5 In the SMTP section, click the CRAM MD-5 or Kerberos checkbox.

6 Click Save.

From the Command Line:

```
# Allow secure SMTP authentication
serveradmin settings mail:postfix:smtpd_sasl_auth_enable = yes
serveradmin settings mail:postfix:smtpd_use_pw_server = "yes"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:0 =
     "gssapi"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:1 =
     "cram-md5"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:2 = "login"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:3 = "plain"
```

Configuring SSL Transport for SMTP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

To configure SSL transport for SMTP connections:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Advanced tab.

4 Select Security.

5 In the SMTP SSL section click Require or Use to enable (or Don't Use to disable).

6 Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.

7 Click Save.

From the Command Line:

```
# Configure SSL transport for SMTP connections
serveradmin settings mail:postfix:smtpd_use_tls = "yes"
```

Using ACLs for Mail Service Access

Access Control Lists (ACLs) are a method of designating service access to specific users or groups on an individual basis. For example, you can use an ACL to allow only one user access to a file server or shell login, without allowing any other user on the server to access it.

Mail services are different from services that traditionally use ACLs for determining service access. Mail service is already specified on a per-user basis. Either you have a mail account on a server or you don't. Being a user on a server doesn't automatically confer access to mail storage and retrieval.

Some administrators find it easier to designate mail access using ACLs if they are doing all their other configuration using ACLs. They also might have mixed network environments that necessitate using ACLs to assign mail access.

Leopard Server allows you to enable mail access for users using the Access tab in a server's Server Admin listing. If you enabled user access via Server Admin and traditional mail access using Workgroup Manager, the settings interact in the following manner:

Access via ACL	Access via Workgroup Manager	Result
On	On	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
On	Off	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
Off	On	User has mail access granted according to his or her user record settings in Workgroup Manager. This is the default.
Off	Off	User has no mail access.

To enable a user's mail access using ACLs:

1. In Server Admin, select the server that has Mail service running and then click Settings.
2. Select Access, then click Services.
3. Select Mail from the Services list.
4. Deselect "Use same access for all services."
5. Select "Allow only users and group below."
6. Click the Add (+) button to reveal a Users and Groups list.
7. Drag the user to the access list.
8. Click Save.

From the Command Line:

```
# Enable a user's mail access using ACLs
dseditgroup -o edit -a $USER -t user com.apple.access_mail
```

Limiting Junk Mail and Viruses

You can configure Mail service to decrease the volume of unsolicited commercial mail, also known as junk mail (or spam), and mail containing viruses. You can take steps to block junk mail or viruses that are sent to mail users. Additionally, you can secure your server against use by mail service abusers, who try to use your resources to send junk mail to others.

You can also prevent senders of junk mail from using your server as a relay point. A relay point or open relay is a server that unselectively receives and forwards mail addressed to other servers. An open relay sends mail from any domain to any domain.

Junk mail senders exploit open relay servers to avoid having their own SMTP servers blacklisted as sources of junk mail. You don't want your server blacklisted as an open relay because other servers may reject mail from your users.

There are two main methods of preventing viruses and junk mail passing through or into your mail system. Using both methods will help ensure your mail system integrity. The two points of control are:

- "Connection Control" on page 261
- "Mail Screening" on page 265

Connection Control

This method of prevention controls which servers can connect to your mail system and what those servers must do to send mail through your mail system. Your mail service can do any of the following to exercise connection control:

- Require SMTP authentication
- Restrict SMTP relay, allowing relay only by approved servers
- Reject all SMTP connections from disapproved servers
- Reject mail from blacklisted servers
- Filter SMTP connections

These methods are explained on the following pages.

Requiring SMTP Authentication

If your Mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server.

Although SMTP authentication applies primarily to mail relay, your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they can't send mail to remote servers. Mail sent from external mail servers and addressed to local recipients is still accepted and delivered.

To require SMTP authentication, see "Enabling Secure SMTP Authentication" on page 258.

Restricting SMTP Relay

Your Mail service can restrict SMTP relay by allowing only approved hosts to relay mail. You create the list of approved servers.

Approved hosts can relay through your Mail service without authenticating. Servers not on the list cannot relay mail through your Mail service unless they authenticate first. All hosts, approved or not, can deliver mail to your local mail users without authenticating.

Your Mail service can log connection attempts made by hosts not on your approved list.

To restrict SMTP relay:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Accept SMTP relays only from these" checkbox.
5. Edit the list of hosts:
 - Click the Add (+) button to add a host to the list.
 - Click the Remove (–) button to delete a selected host from the list.
 - Click the Edit (/) button to change a selected host from the list.

When adding to the list, you can use a variety of notations.

- Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21.
- Enter a host name, such as mail.example.com.
- Enter an Internet domain name, such as example.com.

From the Command Line:

```
# Restrict SMTP relay
serveradmin settings mail:postfix:mynetworks_enabled = yes
```

SMTP Authentication and Restricted SMTP Relay Combinations

The following table describes the results of using SMTP authentication and restricted SMTP relay in various combinations.

SMTP requires authentication	Restricted SMTP relay	Result
On	Off	All mail servers must authenticate before your Mail service accepts mail for relay. Your local mail users must also authenticate to send mail out.
On	On	Approved mail servers can relay without authentication. Servers you haven't approved can relay after authenticating with your Mail service.
Off	On	Your Mail service can't be used for open relay. Approved mail servers can relay (without authenticating). Servers that you haven't approved can't relay unless they authenticate, but they can deliver to your local mail users. Your local mail users don't need to authenticate to send mail. This is the most common configuration.

Rejecting SMTP Connections from Specific Servers

Your Mail service can reject unauthorized SMTP connections from hosts on a disapproved-hosts list that you create. Mail traffic from hosts on this list is denied and SMTP connections are closed after posting a 554 SMTP connection refused error.

To reject unauthorized SMTP connections from specific servers:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Refuse all messages from these" checkbox.
5. Edit the list of servers:
 - Click the Add (+) button to add a host to the list.
 - Click the Remove (–) button to delete the selected host from the list.
 - Click the Edit (/) button to change the selected host from the list.

 When adding to the list, you can use the following notations:
 - Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21.
 - Enter a host name, such as mail.example.com.
 - Enter an Internet domain name, such as example.com.

From the Command Line:

```
# Reject unauthorized SMTP connections
serveradmin settings mail:postfix:smtp_reject_list_enabled = yes
serveradmin settings mail:postfix:smtp_reject_list:_array_index:0 =
     "$NETWORK"
```

Rejecting Mail from Blacklisted Senders

Your Mail service can reject mail from SMTP servers that are blacklisted as open relays by a Real-time Blacklist (RBL) server. Your Mail service uses an RBL server that you specify. RBLs are also called *black-hole servers*.

Blocking unsolicited mail from blacklisted senders might not be completely accurate. Sometimes it prevents valid mail from being received.

To reject mail from blacklisted senders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Use these junk mail rejection servers" checkbox.
5. Edit the list of servers by adding the DNS name of an RBL server:
 - Click the Add (+) button to add a server to the list, then enter the domain name of a RBL server, such as rbl.example.com.
 - Click the Remove (–) button to delete the selected server from the list.
 - Click the Edit (/) button to change the selected server.

From the Command Line:

```
# Reject mail from blacklisted senders
serveradmin settings mail:postfix:black_hole_domains:_array_index:0 =
     "$BLACKLIST_SERVER"
serveradmin settings mail:postfix:maps_rbl_domains_enabled = yes
```

Filtering SMTP Connections

You can use Firewall service of Leopard Server to allow or deny access to your SMTP Mail service from specific IP addresses. Filtering disallows communication between an originating host and your mail server. Mail service doesn't receive the incoming connection and no SMTP error is generated or sent back to the client.

To filter SMTP connections:

1. In Server Admin, select Firewall in the Computers & Services pane.
2. Create a firewall IP filter using the instructions in *Network Services Administration,* using the following settings:
 - Access: denied
 - Port number: 25 (or your incoming SMTP port, if you use a nonstandard port)
 - Protocol: TCP
 - Source: the IP address or address range you want to block
 - Destination: your mail server's IP address
3. If needed, log the packets to monitor the SMTP abuse.
4. Add more filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information about Firewall service, see *Network Services Administration*.

Mail Screening

After a mail delivery connection is made and the message is accepted for local delivery (relayed mail is not screened), the mail server can screen it before delivery. Leopard Server uses SpamAssassin (from spamassassin.apache.org) to analyze the text of a message, and gives it a probability rating for being junk mail.

No junk mail filter is 100% accurate in identifying unwanted mail. For this reason the junk mail filter in Leopard Server doesn't delete or remove junk mail from being delivered. Instead, it marks the mail as potential junk mail.

The user can then decide if it's really unsolicited commercial mail and deal with it accordingly. Many mail clients use the ratings that SpamAssassin adds as a guide in classifying mail for the user.

Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can deal with it in several ways, as described in "Enabling Junk Mail Screening (Bayesian Filters)" on page 265. Virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

Enabling Junk Mail Screening (Bayesian Filters)

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

Bayesian mail filtering is the classification of mail messages based on statistics. Each message is analyzed and word frequency statistics are saved. Mail messages that have more of the same words as those in junk mail receive a higher marking of probability that they are also junk mail. When the message is screened, the server adds a header ("X-Spam-Level") with the junk mail probability score.

For example, let's say you have 400 mail messages where 200 of them are junk mail and 200 are good mail. When a message arrives, its text is compared to the 200 junk mail and the 200 good messages. The filter assigns the incoming message a probability of being junk or good, depending on what group it most resembles.

Bayesian filtering has shown itself to be a very effective method of finding junk mail, if the filter has enough data to compare. One of the strengths of this method is the more mail you get and classify (a process called training), the more accurate the next round of classification is. Even if junk mail senders alter their mailings, the filter takes that into account the next time around.

To enable junk mail screening:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Mail for Junk Mail.
5. Set the level of permissiveness (Cautious, Moderate, Aggressive).

 The permissiveness meter sets how many junk mail flags can be applied to a message before it is processed as junk mail. If you set it to "Least permissive," mildly suspicious mail is tagged and processed as junk mail. If you set it to "Most permissive" it takes a high score (in other words, many junk mail characteristics) to mark it as junk.
6. Decide how to deal with junk mail messages.
 - *Bounced*: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
 - *Deleted*: Deletes the message without delivery. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
 - *Delivered*: Delivers the message even though it's probably junk mail. You can optionally add text to the subject line, indicating that the message is probably junk mail, or encapsulate the junk mail as a MIME attachment.
 - *Redirected*: Delivers the message to someone other than the intended recipient.
7. Choose how often to update the junk mail database updated, if desired.
8. Click Save.

For an explanation of other options, see "Filtering Mail by Language and Locale" on page 268.

From the Command Line:

```
# Enable junk mail screening
serveradmin settings mail:postfix:spam_scan_enabled = yes
```

Manually Training the Junk Mail Filter

It's important to teach the filter what is and what isn't junk mail. Initially, the filter won't be very accurate at marking junk mail, but you can train it to do better. Accurate training requires a large sample, so a minimum of 200 messages of each type is advised.

To train the filter:

1. Choose a mailbox of 200 messages made of only junk mail.
2. Use Terminal and the filter's command-line training tool to analyze it and remember it as junk mail using the following command:

   ```
   sa-learn --showdots --spam <junk mail directory>/*
   ```

3. Choose a mailbox of 200 messages made of only good mail.
4. Use Terminal and the filter's command-line training tool to analyze it and remember it as good mail using the following command:

   ```
   sa-learn --showdots --ham <junk mail directory>/*
   ```

If the junk mail filter fails to identify a junk mail message, train it again so it can do better next time. Use `sa-learn` again with the `--spam` argument on the mislabeled message. Likewise, if you get a false positive (a good message marked as junk mail), use `sa-learn` again with the `--ham` argument to further train the filter.

From the Command Line:

```
# Train the filter
sa-learn --showdots --spam $JUNK_DIRECTORY/*
sa-learn --showdots --ham $NON_JUNK_DIRECTORY/*
```

Automatically Training the Junk Mail Filter

The junk mail filter must be told what is and isn't junk mail. Leopard Server provides a method of automatically training the filter with the help of mail users. The server runs an automated command at 1 am (a cron job) that scans two specially named mail users' in boxes. It runs SpamAssassin's sa-learn tool on the contents of the in boxes and uses the results for its adaptive junk mail filter.

To automatically train the junk mail filter:

1. Enable junk mail filtering.

 See "Enabling Junk Mail Screening (Bayesian Filters)" on page 265.

2. Create two local accounts: junkmail and notjunkmail.
3. Use Workgroup Manager to enable them to receive mail.
4. Instruct your mail users to redirect junk mail messages that have not been tagged as junk mail to junkmail@<yourdomain>.
5. Instruct your mail users to redirect real mail messages that were wrongly tagged as junk mail to notjunkmail@<yourdomain>.

 Each day at 1 am, the junk mail filter will learn what is junk and what was mistaken for junk, but is not.

6. Delete the messages in the junkmail and notjunkmail accounts daily.

From the Command Line:

```
# Automatically train the junk mail filter
/etc/mail/spamassassin/learn_junk_mail
```

Filtering Mail by Language and Locale

You can filter incoming mail based on locales or languages. Mail messages composed in foreign text encodings are often erroneously marked as junk mail. You can configure your mail server to not mark messages from designated originating countries or languages as junk mail.

To allow mail by language and locale:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Junk Mail.
5. Click the Edit (/) button next to Accepted Languages to change the list, select the language encodings to allow as non-junk mail, and click OK.

6 Click the Edit (/) button next to Accepted Locales to change the list, select the country codes to allow as non-junk mail, and click OK.

7 Click Save.

From the Command Line:

```
# Allow mail by language and locale
serveradmin settings mail:postfix:spam_ok_languages = "en fr de"
serveradmin settings mail:postfix:spam_ok_locales = "en"
```

Enabling Virus Screening

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can choose to deal with it several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

To enable virus screening:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Filters tab.

4 Select Scan Email for Viruses.

5 Decide how to deal with messages containing viruses.

Bounced: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account (probably the domain's postmaster) and notify the intended recipient.

Deleted: Deletes the message without delivery. You can optionally send a mail notification to some mail account, probably the postmaster, as well as the intended recipient.

Quarantined: Delivers the message to a directory for further analysis. You can optionally send a mail notification of the quarantine to some mail account, probably the postmaster.

6 Choose if you want to notify the intended recipient if the message was filtered.

7 Choose how often to update the virus database.

A minimum of twice a day is suggested. Some administrators choose eight times a day.

8 Click Save.

From the Command Line:

```
# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes
```

Viewing Mail Service Logs

Mail service maintains the following logs that you can view in Server Admin. The file location for each log is shown beneath the Show pop-up menu.

- *Mail Access:* General mail service information goes into this log.
- *IMAP log:* IMAP-specific activity goes into this log.
- *POP log:* POP specific activity goes into this log.
- *SMTP log:* SMTP specific activity goes into this log.
- *Mailing List logs:* The logs record Mailmain's activity, including service, error, delivery failures, postings, and subscriptions.
- *Junk Mail and Virus logs:* These show activity for mail filtering, including logs for virus definition updates (freshclam log), virus scanning (clamav log), and mail filtering (amavis log).

Logs can be refined by using the text filter box in the window.

To view a Mail service log:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click the Logs button.
3. From the View pop-up menu choose a log type.
4. Click Save.

From the Command Line:

```
# View a Mail service log
tail /var/log/mail.log
```

Securing Antivirus Services

18

Use this chapter to learn how to use the antivirus services built into your system to detect and remove viruses.

Installing antivirus tools helps prevent infection of your computer by viruses, and helps prevent your computer from becoming a host for spreading viruses to other computers. These tools quickly identify suspicious content and compare them to known malicious content.

Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages and attachments for viruses. If a suspected virus is found, ClamAV deletes the message or quarantines it to a specified directory on the server for further analysis.

The virus definitions are kept up to date (if enabled) via the Internet using a process called `freshclam`.

In addition to using antivirus tools, you should develop computer usage habits that prevent virus infection. For example, don't download or open content you didn't specifically request, and never open a file sent to you by someone you don't know.

When you use antivirus tools, make sure you have the latest virus definition files. The protection provided by your antivirus tool depends on the quality of your virus definition files. If your antivirus tool supports it, enable automatic downloading of virus definitions.

For a list of antivirus tools, see the *Macintosh Products Guide* at guide.apple.com.

Securely Configuring and Managing Antivirus Services

This section describes how to securely configure and manage antivirus services.

Enabling Virus Scanning

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

To enable virus screening:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Viruses.
5. Decide how to deal with junk mail messages.

 Bounced: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account (probably the domain's postmaster) and notify the intended recipient.

 Deleted: Deletes the message without delivery. You can optionally send a mail notification to some mail account, probably the postmaster, as well as the intended recipient.

 Quarantined: Delivers the message to a directory for further analysis. You can optionally send a mail notification of the quarantine to some mail account, probably the postmaster.
6. Choose if you want to notify the intended recipient if the message was filtered.
7. Choose how often to update the virus database.

 A minimum of twice a day is suggested. Some administrators choose eight times a day.
8. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Antivirus Services
# ------------------------------------------------------------------

# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes
```

Managing ClamAV with ClamXav

You can use ClamXav, a free GUI front-end to the ClamAV open source virus checker.

This tool allows you to:

- Update virus definitions
- Scan files and folders for viruses

ClamXav performs the following tasks:

- Logs results to a log file
- Places infected files into quarantine
- Monitors folders for changes to their contents

You can access ClamXav services through contextual pop-up menus in the Finder.

Viewing Antivirus Services Logs

Mail service maintains the following junk mail and virus logs that you can view in Server Admin. The file location for each log is shown beneath the Show pop-up menu.

- Junk Mail/Virus Scanning (/var/log/amavis.log)
- Virus (/var/log/clamav.log)
- Virus Database Updates (/var/log/freshclam log)

To view a virus service log:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click the Logs button.
3. From the View pop-up menu choose a log type.
4. Click Save.

From the Command Line:

```
# View a virus log
tail /var/log/amavisd.log
```

Securing File Services

19

Use this chapter to learn how to secure File services.

Securely configuring File services is an important step in the process of protecting your private data from network attacks.

Leopard Server's cross-platform file sharing services help groups work more efficiently by letting them share resources, archive projects, exchange and back up important documents, and conduct other file-related activities.

Sharing files over a network opens your computers up to a host of vulnerabilities. With File services enabled, you are allowing access to files and folders on your server (also called share points).

For more information about configuring File services, see the *File Services Administration* guide.

Security Considerations

The most effective method of securing your network is to assign correct privileges for each file, folder, and share point you create.

Restricting Access to File Services

Use Service Access Control Lists (SACLs) to restrict access to AFP, FTP, and SMB services.

Restricting Access to Everyone

Be careful when creating and granting access to share points, especially if you're connected to the Internet. Granting access to Everyone or to World (in NFS service) could expose your data to anyone on the Internet. For NFS, it is recommended that you do not export volumes to World and that you use Kerberos to provide security for NFS volumes.

Restricting Access to NFS Share Points

NFS share points without the use of Kerberos don't have the same level of security as AFP and SMB, which require user authentication (entering a user name and password) to gain access to a share point's contents.

If you have NFS clients, consider setting up a share point to be used only by NFS users, or configure NFS with Kerberos. NFS doesn't support SACLs. For more information, see "Protocol Security Comparison" on page 276.

Restricting Guest Access

When you configure file service, you can turn on guest access. Guests are users who connect to the server anonymously without entering a user name or password. Users who connect anonymously are restricted to files and folders that have privileges set to Everyone.

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, take the following precautions by using File Sharing in Server Admin:

- Depending on the controls you want to place on guest access to a share point, consider the following options:
 - Set privileges for Everyone to None for files and folders that guest users shouldn't access. Items with this privilege setting can be accessed only by the item's owner or group.
 - Put files available to guests in one folder or set of folders and then assign the Read Only privilege to the Everyone category for that folder and each file in it.
 - Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder.
- Don't export NFS volumes to World. Restrict NFS exports to a subnet or a specific list of computers.
- Disable access to guests or anonymous users over AFP, FTP, and SMB using Server Admin.
- Share individual folders instead of entire volumes. The folders should contain only those items you want to share.

Restricting File Permissions

Before a folder is shared, its permissions should be restricted as much as possible. Permissions on share points set as user home folders are particularly important. By default, users' home folders are set to allow any other user to read their contents.

For more information about setting file permissions, see Chapter 6, "Securing System Preferences," on page 112.

Protocol Security Comparison

When sharing network resources, configure your server to provide the necessary security.

AFP and SMB provide some level of encryption to secure password authentication. AFP and SMB do not encrypt data transmissions over the network so you should only use them on a securely configured network.

FTP does not provide password or data encryption. When using this protocol, make sure your network is securely configured. Instead of using FTP, consider using the `scp` or `sftp` command-line tools. These tools securely authenticate and securely transfer files.

The following table provides a comparison of the protocols and their authentication and encryption capabilities.

Protocol	Authentication	Data Encryption
AFP	Cleartext and encrypted (Kerberos) passwords.	Not encrypted and data is visible during transmission.
NFS	Encrypted (Kerberos) password and system authentication.	Can be configured to encrypt data transmission.
SMB	Cleartext and encrypted (NTLM v1, NTLM v2, LAN Manager, and Kerberos) passwords.	Not encrypted and data is visible during transmission.
FTP	Cleartext passwords.	Not encrypted. Data is sent as cleartext.

Disabling File Services

Unless you use the server as a file server, disable file sharing services. Disabling these services prevents your computer from being used by an attacker to access other computers on your network.

To disable file sharing services:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect AFP, FTP, NFS, SMB.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing File Services
# ------------------------------------------------------------------

# Disable file sharing services
serveradmin stop afp
serveradmin stop smb
serveradmin stop ftp
serveradmin stop nfs
```

Choosing a File Sharing Protocol

If you require file sharing services, you must choose which file sharing protocols are needed before configuring your services. The protocol is configured for the folders you are sharing, called share points. The share points are created and configured using Workgroup Manager.

Most installations only need one file sharing protocol, and you should use as few protocols as possible. Limiting the number of protocols used by a server limits its exposure to vulnerabilities discovered in those protocols. The protocol choices are:

- Apple Filing Protocol (AFP)—AFP is the preferred method of file sharing for Macintosh or compatible client systems. AFP supports authentication of clients, and also supports encrypted network transport using SSH.
- File Transfer Protocol (FTP)—FTP should generally not be used for file sharing. Use the SFTP feature of SSH instead. SFTP provides a secure means of authentication and data transfer, while FTP does not.

 The only situation where FTP is acceptable is when the server must act as a file server for anonymous users. This might be necessary over wide area networks, where there is no concern for the confidentiality of data and responsibility for the integrity of the data rests with its recipient.
- Network File System (NFS)—NFS is a common file sharing protocol for UNIX computers. Avoid using NFS, because it does not perform authentication of its clients—it grants access based on client IP addresses and file permissions. Using NFS may be appropriate if the client computer administration and the network are trusted.

- Microsoft Windows Server Message Block (SMB)—SMB is the native file sharing protocol for Microsoft Windows. Avoid using SMB—it supports authentication but does not support encrypted network transport, and it uses NTLMv1 and NTLMv2 encryption, both of which are weak password hashing schemes. SMB may be an appropriate protocol for Windows clients when the network between the server and client is not at risk for eavesdropping.

Each protocol is appropriate for specific situations. Deciding which protocol to use depends on the clients and networking needs. After you choose a protocol for file sharing, you must configure the file sharing protocol.

If no share points are shared with a protocol, disable the service that runs that protocol using Server Admin. The NFS service automatically stops when no share points specify its use.

Configuring AFP File Sharing Service

Apple File Service, which uses AFP, lets you share files among Macintosh clients. Because it provides authentication and encryption, AFP service is the preferred file sharing method for Macintosh or compatible clients.

Note: Encryption does not apply to automatically mounted home folders, where only authentication is provided.

To securely configure AFP Service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings. Click General.
5. Deselect "Enable Bonjour registration."
6. Enter the login greeting according to site policy.
7. Click Access.
8. For Authentication, choose "Kerberos" if your system is integrated into a Kerberos system; otherwise, choose "Standard."
9. Deselect "Enable administrator to masquerade as any registered user."
10. Under Maximum Connections, enter the largest expected number for Client Connections.
11. Although you'll disable Guest access, enter "1" for Guest Connections to minimize exposure in case it is accidentally reenabled.
12. Deselect "Enable Guest access."

13 Click Logging.

14 Select "Enable access Log" to enable logging.

15 Select "Archive every __ day(s)" and set the frequency to three days or according to your organization's requirements.

16 Select "Login" and "Logout" to include events in the access log.

If you need stronger accounting, select the other events.

17 Under Error Log, select "Archive every __ day(s)" and set the frequency to three days or according to your organization's requirements.

18 Click Idle Users and configure Idle Users settings:

- Deselect "Allow clients to sleep __ hour(s) - will not show as idle."
- Select "Disconnect idle users after __ minute(s)" and enter a value in the text field to mitigate risk from a computer accidentally being left unattended.
- Deselect Guests, Administrators, Registered Users, and Idle Users who have open files.
- Enter a "Disconnect Message" notice according to site policy.

19 Click Save.

20 Click Start AFP (below the Servers list).

21 For additional security enhancements, further restrict AFP by using SACLs and firewall rules.

These are configured based on your organization's network environment:

- You can configure SACLs to restrict AFP access to specific users or groups. For more information, see "Setting Service Access Control Lists" on page 205.
- You can configure firewall rules that prevent AFP connections from unintended sources. For more information, see "Creating Firewall Service Rules" on page 233.

From the Command Line:

```
# Securely configure AFP Service
serveradmin settings afp:registerNSL = no
serveradmin settings afp:attemptAdminAuth = no
serveradmin settings afp:clientSleepOnOff = no
serveradmin settings afp:idleDisconnectOnOff = yes
serveradmin settings afp:authenticationMode = "kerberos"
serveradmin settings afp:activityLog = yes
serveradmin settings afp:guestAccess = no
```

Configuring FTP File Sharing Service

If authentication of users is possible, use the SFTP portion of SSH instead of FTP to securely transmit files to and from the server. For more information, see "Transferring Files Using SFTP" on page 213.

FTP is acceptable only if its anonymous access feature is required, which allows unauthenticated clients to download files. The files are transferred unencrypted over the network and no authentication is performed.

Although the transfer does not guarantee confidentiality or integrity to the recipient, it may be appropriate in some cases. If this capability is not specifically required, disable it.

To configure FTP to provide anonymous FTP downloads:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click General.
5. In "Disconnect client after __ login failures," enter 1.

 Even though authenticated connections are not accepted, logins should fail quickly if accidentally activated.
6. Enter a mail address specially set up to handle FTP administration—for example, ftpadmin@hostname.com.
7. Under Access, select "Kerberos" for Authentication.

 If a Kerberos server is not set up, the authentication process is blocked.
8. In "Allow a maximum of __ authenticated users," enter 1.

 The GUI does not allow setting this to 0, but authenticated users are disabled in later steps.
9. Select "Enable anonymous access."

 Anonymous access prevents the user credentials from being sent openly over the network.

 Important: Before selecting this option, review the privileges assigned to your share points under File Privileges in the Sharing pane to make sure there are no security holes.

 Anonymous users can log in using the name "ftp" or "anonymous." They do not need a password to log in, but they are prompted to enter their mail addresses.
10. Determine a maximum number of anonymous users and enter the number in "Allow a maximum of __ anonymous users."

11 Under File conversion, deselect "Enable MacBinary and disk image auto-conversion."

12 Click Messages.

13 Select "Show Welcome Message" and enter a welcome message according to site policy.

14 Select "Show Banner Message" and enter a banner message according to site policy.

Do not reveal software information, such as operating system type or version, in the banner.

15 Click Logging.

16 Select all options under "Log Authenticated Users" and "Log Anonymous Users."

Even though authenticated users are not allowed to log in, their attempts should be logged so corrective action can be taken.

17 Click Advanced.

18 Set "Authenticated users see" to FTP Root and Share Points.

Authenticated users and anonymous users see the same FTP root.

19 Verify that "FTP root" is set to the /Library/FTPServer/FTPRoot/ folder.

20 Click Save.

21 Click Start FTP (below the Servers list).

22 Open the /Library/FTPServer/FTPRoot/ folder and drag the contents (Users, Groups, Public) to the trash.

23 Drag the files to share with anonymous users to the /Library/FTPServer/FTPRoot/ folder.

24 Verify that the file permissions for the /Library/FTPServer/FTPRoot/ folder do not allow public write access.

25 Open the file /Library/FTPServer/Configuration/ftpaccess for editing.

26 Delete lines that begin with "upload."

The following two line are present by default:

```
upload /Library/FTPServer/FTPRoot /uploads yes ftp daemon 0666 nodirs
upload /Library/FTPServer/FTPRoot /uploads/mkdirs yes ftp daemon 0666 dirs
     0777
```

27 Insert the following line to prevent advertisement of operating system and version information:

```
greeting terse
```

28 Insert the following lines to prevent users from authenticating.

```
deny-gid %-99 %65535
deny-uid %-99 %65535
allow-gid ftp
allow-uid ftp
```

This forces users to access FTP anonymously, protecting their login credentials.

29 For additional security enhancements, you can further restrict the FTP service by using SACLs and firewall rules.

These are configured based on your organization's network environment.

- You can configure SACLs to restrict FTP access to specific users or groups. For more information about configuring SACLs, see "Setting Service Access Control Lists" on page 205.
- You can configure firewall rules that prevent FTP connections from unintended sources. For more information, see "Creating Firewall Service Rules" on page 233.

From the Command Line:

```
# Configure FTP to provide anonymous FTP downloads
serveradmin settings ftp:logSecurity:anonymous = yes
serveradmin settings ftp:logSecurity:guest = yes
serveradmin settings ftp:logSecurity:real = yes
serveradmin settings ftp:maxRealUsers = 1
serveradmin settings ftp:enableMacBinAndDmgAutoConversion = no
serveradmin settings ftp:authLevel = "KERBEROS"
serveradmin settings ftp:anonymousAccessPermitted = yes
serveradmin settings ftp:bannerMessage = "$BANNER"
serveradmin settings ftp:maxAnonymousUsers = 500
serveradmin settings ftp:administratorEmailAddress = "user@domain.com"
serveradmin settings ftp:logCommands:anonymous = yes
serveradmin settings ftp:logCommands:guest = yes
serveradmin settings ftp:logCommands:real = yes
serveradmin settings ftp:loginFailuresPermitted = 1
serveradmin settings ftp:welcomeMessage = "$WELCOME"
```

Configuring NFS File Sharing Service

NFS does not support user name and password authentication. It relies on client IP addresses to authenticate users, and on client enforcement of permissions. This is not a secure approach in most networks. Therefore, use NFS only if you are on a LAN with trusted client computers, or if you are in an environment that can't use Apple file sharing or Windows file sharing.

The NFS server included with Leopard Server lets you limit access to a share point based on a client's IP address. Restrict access to a share point exported using NFS to those clients that require it. You can reshare NFS mounts using AFP, Windows, and FTP so that users can access NFS volumes in a more restricted fashion.

To configure and start NFS service, use Server Admin. For information about how to setup and restrict NFS service, see "NFS Share Points" on page 183.

For additional security enhancements, you can further restrict the NFS service by using firewall rules. You can configure firewall rules that prevent AFP connections from unintended sources.

For more information, see "Creating Firewall Service Rules" on page 233. Rules are configured based on your organization's network environment.

Configuring SMB File Sharing Service

If share points need to use SMB, activate Windows file service and configure it. Support for SMB is provided by the open source Samba project, which is included with Leopard Server.

SMB uses NTLMv1 and NTLMv2 encryption, which are very weak password hashing schemes. For more information about configuring the Samba software, go to www.samba.org.

To securely configure Windows file sharing service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings. Click General.
5. Choose the Role according to operational needs.

 If the server shares files but does not provide authentication services, "Standalone Server" is the relevant choice.
6. Fill in the text fields appropriately, leaving the Description field blank.

 It is helpful for the computer name to match the host name (without the domain name). The Workgroup name depends on the configuration of Windows domains on your subnet.
7. Click Access.
8. Deselect "Allow Guest access."

9 For "Client connections," select "__ maximum" and enter the maximum number of client connections expected.

The Graphs pane can display the actual usage, which can help you adjust the number for your network.

10 Click Logging.

11 Change "Log Detail" to at least "medium" to capture authentication failures.

12 Click Advanced.

13 Under Services, deselect "Workgroup Master Browser" and "Domain Master Browser" unless these services are required.

14 Select Off for WINS registration.

15 Click Save.

16 Click Start SMB (below the Servers list).

17 For additional security enhancements, you can further restrict the Windows service by using SACLs and firewall rules.

These are configured based on your organizations network environment:

- You can configure SACLs to restrict Windows access to specific users or groups. For more information about configuring SACLs, see "Setting Service Access Control Lists" on page 205.
- You can configure firewall rules that prevent Windows connections from unintended sources. For more information, see "Creating Firewall Service Rules" on page 233.

From the Command Line:

```
# Securely configure Windows file sharing service
serveradmin settings smb:wins support = no
serveradmin settings smb:domain master = no
serveradmin settings smb:map to guest = "Never"
serveradmin settings smb:auth methods = "odsam"
serveradmin settings smb:ntlm auth = "no"
serveradmin settings smb:max smbd processes = 1000
serveradmin settings smb:log level = 1
serveradmin settings smb:preferred master = no
serveradmin settings smb:os level = 65
```

Securing Web Service

20

Use this chapter to learn how to secure Web service.

Web service provides an easy method of accessing data from anywhere in the world. However, this access is often attacked due to its weakness on other platforms. Leopard Server provides many configuration options to protect Web service.

Web service is based on Apache, an open source HTTP web server. A web server responds to requests for HTML webpages stored on your site. Open source software gives you the capability to view and change the source code to make changes and improvements. This has led to Apache's widespread use, making it one of the most popular web servers on the Internet today.

Web administrators can use Server Admin to administer Web service without knowing about advanced settings or configuration files. Web administrators proficient with Apache can also administer web technologies using Apache's advanced features.

Because Web service in Leopard Server is based on Apache, you add advanced features with plug-in modules. Apache modules let you add support for Simple Object Access Protocol (SOAP), Java™, and CGI languages such as Python.

Fore more information about the Apache project, see www.apache.org. The Center for Internet Security (CIS) at www.cisecurity.org provides an Apache Benchmark and Scoring tool. CIS Benchmarks enumerate security configuration settings and actions that harden your computer.

For more information about configuring web service, see the *Web Technologies Administration* guide.

Disabling Web Service

If the system is not intended to be a web server, disable web server software.

Secure web administration demands scrutiny of configuration settings. Use SSL encryption to encrypt sensitive web traffic.

If the system is not intended to be a web server, disable Web services using the Server Admin tool.

Disabling the service prevents potential vulnerabilities on your computer. Web service is disabled by default, but verification is recommended.

To disable Web service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect Web.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Web Service
# ------------------------------------------------------------------

# Disable Web service
serveradmin stop web
```

Managing Web Modules

If your system does not require active web modules, disable them. Web modules (sometimes called plug-ins) consist of web components that add functionality to Web service. Using unnecessary modules creates potential security risks when the Web service is running.

Many types of web modules are available for use with Web service. Verify that each module used is required and that you understand the impact it has to security when Web service is running.

Important: When disabling web modules, make sure the module is not needed by another web service you are running. If you disable a web module that another web service is dependent on, that web service might not work.

To disable web modules:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.
4. Click Settings, then click Modules.
5. Deselect all modules except for the modules your site requires.
6. Click Save.

Disabling Web Options

Disable the following web options unless they are specifically required for web services. Activating these options enables their associated web modules. This can be a security risk if you don't understand the impact the module has to security when a web service is running.

Disable the following web modules unless they are specifically required for a web service:

- **Folder Listing:** Displays a list of folders when users specify the URL and no default webpage (such as index.html) is present. Instead of viewing a default webpage, the server shows a list of the web folder's contents. Folder listings appear only if no default document is found.
- **WebDAV:** Turns on Web-based Distributed Authoring and Versioning (WebDAV), which allows users to make changes to websites while the sites are running. If you enable WebDAV you must also assign access privileges for the sites and for the web folders.
- **CGI Execution:** Permits Common Gateway Interface (CGI) programs or scripts to run on your web server. CGI programs or scripts define how a web server interacts with external content-generating programs.
- **Server Side Includes (SSI):** Permits SSI directives placed in webpages to be evaluated on the server while the website is active. You can add dynamically generated content to your webpages while the files are being viewed by users.
- **Allow All Overrides:** Instructs Web service to look for additional configuration files inside the web folder for each request.
- **Spotlight Searching:** Allows web browsers to search the content of your website.

To disable web options:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.

3 From the expanded Servers list, select Web.

4 Click Sites, then select the website in the list.

5 Click Options below the websites list.

Deselect Folder Listing, WebDAV, CGI Execution, Server Side Includes (SSI), and Allow All Overrides unless they are required.

From the Command Line:

```
# Disable web options
serveradmin settings web:Modules:_array_id:authz_host_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_fs_module:enabled = no
serveradmin settings web:Modules:_array_id:apple_spotlight_module:enabled =
     no
serveradmin settings web:Sites:_array_id:$SITE:SpotlightIndexing = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
     Library/WebServer/Documents:AllowOverride = "None"
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
     Library/WebServer/Documents:IfModule:_array_id:mod_dav.c:DAV = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
     Library/WebServer/Documents:Options:Includes = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
     Library/WebServer/Documents:Options:ExecCGI = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
     Library/WebServer/Documents:Options:Indexes = no
serveradmin settings web:Sites:_array_id:default_default:SpotlightIndexing
     = no
```

Using Realms to Control Access

You can use realms to control access and provide security to locations or folders in a website. Realms are locations at the URL or files in the folder that users can view.

If WebDAV is enabled, users with authoring privileges can also change content in the realm. You set up the realms and specify the users and groups that have access to them.

When an assigned user or group possesses fewer permissions than the permissions assigned to user Everyone, that user or group is deleted upon a refresh. This happens because the access assigned to Everyone preempts the access assigned to specific users or groups with fewer permissions than those possessed by Everyone. The greater permissions always take precedence.

Consequently, the list of assigned users and groups with fewer permissions are not saved in the Realms pane upon refresh if their permissions are determined to be preempted by the permissions assigned to Everyone. After the refresh, the names are no longer listed in the list on the right in the Realms pane. Also, for a brief period of time, user Everyone will switch its displayed name to "no-user."

To use a realm to control website access:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.
4. Click Sites, then select the website in the list.
5. Below the websites list click Realms.
6. Click the Add (+) button to create a realm.

 The realm is the part of the website users can access.
7. In the Realm Name field, enter the realm name.

 This is the name users see when they log in to the website.
8. From the Authentication pop-up menu, choose a method of authentication:
 - **Basic authentication** is on by default. It is recommended not to use basic authentication for sensitive data because it sends your password to the server unencrypted.
 - **Digest authentication** is more secure than basic authentication because it uses an encrypted hash of your password.
 - **Kerberos authentication** is the most secure because it implements server certificates to authenticate. If you want Kerberos authentication for the realm, you must join the server to a Kerberos domain.
9. Enter the realm location or folder you are restricting access to:

 Choose Location from the pop-up menu and enter a URL to the location in the website that you want to restrict access to.

 Choose Folder from the pop-up menu and enter the path to the folder that you want to restrict access to.

 You can also click the Browse button to locate the folder you want to use.
10. Click OK.
11. Select the new realm and click Add (+) to open the Users & Groups panel.

 To switch between the Users list and the Groups list, click Users or Groups in the panel.

 Use the Realms pane to delete a user or group by selecting the name and clicking the Delete (–) button.

12 To add users or groups to a realm, drag users to the list on the right in the Realms pane.

When users or members of a group you've added to the realm connect to the site, they must supply their user name and password.

13 Limit realm access to specified users and groups by setting the following permissions using the up and down arrows in the Permissions column.

- **Browse Only:** Permits users or groups to browse the website.
- **Browse and Read WebDAV:** Permits users or groups to browse the website and also read the website files using WebDAV.
- **Browse and Read/Write WebDAV:** Permits users or groups to browse the website and also read and write to website files using WebDAV.
- **None:** Prevents users or groups from using permissions.

14 Click Save.

Enabling Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) provides security for a site and its users by authenticating the server, encrypting information, and maintaining message integrity.

SSL is a per-site setting that lets you send encrypted, authenticated information across the Internet. For example, if you want to permit credit card transactions through a website, you can protect the information that's passed to and from that site.

The SSL layer is below application protocols (for example, HTTP) and above TCP/IP. This means that when SSL is operating on the server and on the client computer, all information is encrypted before being sent.

The Apache web server in Leopard Server uses a public key-private key combination to protect information. A browser encrypts information using a public key provided by the server and only the server has a private key that can decrypt that information.

The web server supports SSLv2, SSLv3, and TLSv1. More information about these protocol versions is available at www.modssl.org.

When SSL is implemented on a server, a browser connects to it using the https prefix in the URL, rather than http. The "s" indicates that the server is secure.

When a browser initiates a connection to an SSL-protected server, it connects to a specific port (443) and sends a message that describes the encryption ciphers it recognizes. The server responds with its strongest cipher, and the browser and server then continue exchanging messages until the server determines the strongest cipher that it and the browser can recognize.

The server then sends its certificate (an ISO X.509 certificate) to the browser. This certificate identifies the server and uses it to create an encryption key for the browser to use. At this point a secure connection is established and the browser and server can exchange encrypted information.

Before you can enable SSL protection for a website, you must obtain the proper certificates. For detailed information about certificates and their management, see *Server Administration*.

To set up SSL for a website:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.
4. Click Sites, then select the website in the list.
5. Click Security below the websites list.
6. In the Security pane, select Enable Secure Sockets Layer (SSL).

 When you turn on SSL, a message appears, noting that the port is changed to 443.
7. In the Certificate pop-up menu, choose the certificate you want.

 If the certificate is protected by a passphrase, the name of the certificate must match the virtual host name. If the names don't match, Web service won't restart.
8. If you choose Custom Configuration or want to edit a certificate, you might need to do the following:
 a. Click the Edit (/) button and supply the information in each field for the certificate.
 b. If you received a ca.crt file from the Certificate Authority (CA), click the Edit (/) button and paste the text from the ca.crt file in the Certificate Authority File field.

 Note: The ca.crt file might be required but might not be sent directly to you. This file must be available on the website of the CA.
 c. In the Private Key Passphrase field, enter a passphrase and click OK.
9. In the "SSL Log File" field, enter the pathname for the folder where you want to keep the SSL log.

 You can also use the Browse button to navigate to the folder.
10. Click Save.
11. Confirm that you want to restart Web service.

Server Admin lets you enable SSL with or without saving the SSL passphrase. If you did not save the passphrase with the SSL certificate data, the server prompts you for the passphrase upon restart but won't accept manually entered passphrases.

Use the Security pane for the site in Server Admin to save the passphrase with the SSL certificate data. For more information, see "Using a Passphrase with SSL Certificates" on page 292.

Using a Passphrase with SSL Certificates

If you manage SSL certificates using Server Admin and you use a passphrase for certificates, Server Admin ensures that the passphrase is stored in the system keychain.

When a website is configured to use the certificate and that web server is started, the getsslpassphrase(8) utility extracts the passphrase from the system keychain and passes it to the web server, as long as the certificate name matches the virtual host name.

If you do not want to rely on this mechanism, you can have the Apache web server prompt you for the passphrase when you start or restart it. Use the `serveradmin` command-line tool to configure this.

To configure Apache to prompt you for a passphrase when it starts:

1. Open Terminal and enter the following command.

```
$ sudo serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL
     PassPhraseDialog=builtin
```

2. Start Apache with the command:

```
$ sudo serveradmin start web
```

3. When prompted, enter the certificate passphrase.

From the Command Line:

```
# configure Apache to prompt you for a passphrase when it starts
serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL
     PassPhraseDialog=builtin
```

Viewing Web Service Logs

Use Server Admin to view the error and access logs for Web service, if you have enabled them. Web service in Leopard Server uses the standard Apache log format, so you can also use a third-party log analysis tool to interpret the log data.

To view logs:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.

4 Click Logs, then choose between an access or error log by selecting the log from the list of logs.

To search for specific entries, use the Filter field in the lower right.

From the Command Line:

```
# View logs
tail /var/log/apache2/access_log
```

From the Command Line

You can also view Web service logs in the /Library/Logs/wikid/ or /var/log/apache2/ folder by using the `cat` or `tail` command in Terminal. For more information, see the Web service chapter of *Command-Line Administration*.

Securing WebDAV

Web service includes support for Web-based Distributed Authoring and Versioning, known as WebDAV. With WebDAV capability, your users can check out webpages, make changes, and then check the pages back in while the site is running. In addition, the WebDAV command set is rich enough that client computers with Leopard installed can use a WebDAV-enabled web server as if it were a file server.

Sharing files over a network opens your computers to a host of vulnerabilities. To reduce the security risk when using WebDAV, assign access privileges for the sites and for the web folders.

To securely configure WebDAV for a site:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select Web.

4 Click Sites, then select the website in the list.

5 Click Options below the websites list.

6 Select the WebDAV checkbox.

This option turns WebDAV on, allowing users to make changes to websites while the sites are running. If you enable WebDAV, you must also assign access privileges for the sites and web folders.

Note: If you turned off the WebDAV module in the Modules pane of Server Admin, you must turn it on again before WebDAV takes effect for a site. This is true even if the WebDAV option is selected in the Options pane for the site. For more about enabling modules, see "Managing Web Modules" on page 286.

7 Click Save.

After WebDAV is turned on, you can use realms to control access to the website. For more information about configuring realms, see "Using Realms to Control Access" on page 288.

Securing Blog Services

A blog is like a diary or journal, with entries that are arranged in the order they were created in. On the other hand, a wiki contains shared content that doesn't appear in chronological order. The type of information you want to put on your site helps determine whether it appears in a wiki or in a blog.

By default, blogs are disabled when you start Web service. Blogs can open your computers up to a host of vulnerabilities. If blogs are not required, disable them.

Disabling Blog Services

If you do not need blog services, disable them.

To disable Blog service:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select Web.

4 Click Sites.

5 In the Sites list, click the site where you want blog service disabled.

6 Click Web Services.

7 In the Services for Groups section, deselect the "Wiki and blog" checkbox.

8 Click Save.

From the Command Line:

```
# Disable Blog service
serveradmin settings web:Sites:_array_id:$SITE:weblog = no
```

Securely Configuring Blog Services

You can enable user and group Blog service on your website. Leopard Server includes a group wiki and a group blog. These are enabled together. Group blogs let users in a group access and post entries to the same blog.

Users can also publish their own personal blog using Web services associated with their server account. This gives users the ability to maintain personal blogs on their own user pages.

To set up Blog service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.
4. Click Sites.
5. In the Sites list, click the site where you want Blog service enabled.

 To maximize the security of user interactions with the server hosting blogs, have users access blogs through a site that has SSL enabled.
6. Click Web Services.
7. In the Services for Groups section, select the "Wiki and blog" checkbox.
8. Click Settings.
9. Click Web Services.
10. Click blogs.
11. From the default Wiki and Blog Theme pop-up menu, choose a theme.

 A theme controls the appearance of a blog. Themes determine the color, size, location, and other attributes of blog elements. Each theme is implemented using a style sheet.

 The default theme is used when a blog is created, but blog owners can change the theme. The default theme also controls the appearance of the blog's front page.
12. Identify a blog folder, used to store blog files.

 By default, blog files are stored in /Library/Collaboration on the computer hosting Blog service. You can click Choose to select a different folder, such as a folder on a RAID device or on another computer.
13. Click Save.
14. Make sure the blog server's Open Directory search path includes directories in which users and group members you want to support with Blog service are defined.

 The *Open Directory Administration* guide explains how to set up search paths. Any user or group member defined in the Open Directory search path can now create and access blogs on the server unless you deny them access to Blog service.

Viewing Blog Service Logs

To check Blog service log entries, see "Viewing Web Service Logs" on page 292.

Securing Tomcat

You use Server Admin or Terminal to disable Tomcat if you don't need it.

To stop Tomcat using Server Admin:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Web.
4. Click Settings, then click General.
5. Deselect the Enable Tomcat checkbox.
6. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Tomcat
# ------------------------------------------------------------------

# Stop Tomcat using Server Admin
/Library/Tomcat/bin/startup.sh stop
```

Securing MySQL

MySQL provides a relational database management solution for your web server. With this open source software, you can link data in tables or databases and provide the information on your website.

Disabling MySQL Service

If you do not need to run MySQL service, disable it in Server Admin.

To turn MySQL service on:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.

5 Click Services.

6 Deselect **MySQL**.

7 Click Save.

From the Command Line:

```
# ----------------------------------------------------------------------
# Securing MySQL
# ----------------------------------------------------------------------

# Turn MySQL service on
serveradmin stop mysql
```

Setting Up MySQL Service

Use MySQL service Settings in Server Admin to specify the database location, to enable network connections, and to set the MySQL root password.

To configure MySQL service settings:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click MySQL.

4 Click Settings.

5 To permit users to access MySQL service select the "Allow network connections" checkbox.

This grants users access to database information through the web server.

6 In the Database location field enter the path to the location of your database.

You can also click the Choose button and browse for the folder you want to use.

7 Click Save.

From the Command Line:

```
# Configure MySQL service settings
serveradmin settings mysql:allowNetwork = yes
```

Viewing MySQL Service and Admin Logs

MySQL service keeps two types of logs, a MySQL service log and MySQL admin logs:

- The MySQL service log records the time of events such as when MySQL service is started and stopped.
- The MySQL admin log records information such as when clients connect or disconnect and each SQL statement received from clients. This log is located at /Library/Logs/MySQL.log.

You can view MySQL service logs using Server Admin.

To view MySQL service logs:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click MySQL.
4. Click Logs.

 Use the Filter field to search for specific entries.

From the Command Line:

```
# View MySQL service logs
tail /Library/Logs/MySQL.log
```

Securing WebObjects

Leopard Server includes the WebObjects run-time libraries and an unlimited deployment license to facilitate developing standards-based web services and Java server applications. You can optionally purchase WebObjects development tools from the Apple Store (store.apple.com), Apple's retail stores, and authorized Apple resellers.

You can set WebObjects to start when the server starts. This ensures that WebObjects modules start after a power failure or after the server shuts down.

For more information and documentation on WebObjects, see www.apple.com/webobjects or developer.apple.com/documentation/WebObjects.

Disabling WebObjects

If your server is not intended to be a WebObjects server, disable the WebObjects service. Disabling the service prevents vulnerabilities on your computer. The WebObjects service is disabled by default, but verification is recommended.

To disable the WebObjects service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect WebObjects.
7. Click Save.

From the Command Line:

```
# ---------------------------------------------------------------------
# Securing WebObjects
# ---------------------------------------------------------------------

# Disable the WebObjects service
serveradmin stop webobjects
```

Securing Client Configuration Management Services

21

Use this chapter to learn how to secure Client Configuration Management services.

Securely configuring client configuration management helps standardize the clients across your network and provides a secure deployment.

By managing preferences for users, workgroups, computers, and computer groups, you can customize the user's experience and restrict user access to only the applications and network resources you choose.

To manage preferences, use the Preferences pane in Workgroup Manager.

Properly set managed preferences help deter users from performing malicious activities. They can also help prevent users from accidentally misusing their computer.

Managing Applications Preferences

Use Applications preferences to allow or restrict user access to applications.

Computers identify applications using one of two methods: digital signatures (used in Leopard or later), and bundle IDs (used in Tiger or earlier, but can be used in Leopard or later).

Digital signatures are much more secure because clever users can manipulate bundle IDs. Workgroup Manager supports the use of both methods.

Use the Applications pane to work with digital signatures. Use the Legacy pane to work with bundle IDs.

Application restrictions depend on which pane you're managing and the version of Mac OS X run by client computers:

- If you manage the Applications pane and your users run Leopard or later, Applications settings take effect and Legacy settings are ignored.
- If you don't manage the Applications pane, Legacy settings take effect for any version of Mac OS X.

- If your users run Tiger or earlier, only Legacy settings take effect.

You can also use settings in Applications preferences to allow only specific widgets in Dashboard or to disable Front Row.

The table below describes what the settings in each Applications pane can do.

Applications preference pane	What you can control
Applications	Access to specific applications and paths to applications using digital signatures (for users of Leopard or later)
Widgets	Allowed Dashboard widgets for users of Leopard
Front Row	Whether Front Row is allowed
Legacy	Access to specific applications and paths to applications using bundle IDs (primarily for users of Tiger or earlier)

Controlling User Access to Applications and Folders

You can use Workgroup Manager to prevent users from launching unapproved applications or applications located in unapproved folders.

In Tiger or earlier, applications were identified by their bundle IDs. If your users have Leopard or later installed, you can use digital signatures to identify applications. Digital signatures are much more difficult to circumvent than a bundle ID.

Workgroup Manager can sign applications that aren't already signed. When signing an application, you can embed a signature or you can store a detached signature separately from the application.

Embedding a signature has several performance benefits over a detached signature, but with signature embedding you must make sure every computer has the same signed application. For applications run from a CD, DVD, or other read-only media, you must use detached signatures.

Workgroup Manager uses the following icons to denote the kind of signature associated with an application.

Icon	Indicates the application has this type of signature
(no icon)	Embedded signature
	Detached signature
	No signature

Applications that include helper applications are denoted by a disclosure triangle. When you click the disclosure triangle, you'll see a list of helper applications. By default, these helper applications are allowed to open.

You can disable individual helper applications, but the application might behave erratically if it requires the helper applications.

To allow or prevent users from launching an application, add the application or application path to one of three lists:

- **Always allow these applications.** Add applications that should always be allowed, regardless of their inclusion in other lists. You can sign applications added to this list. It is recommended not to add unsigned applications to this list because they allow users to disguise unapproved applications as approved applications.
- **Disallow applications within these folders.** Add applications and folders containing applications you want to prevent users from opening. All applications in the subfolders of a disallowed folder are also disallowed. Disallowing a folder in an application package can cause the application to behave erratically or fail to load.
- **Allow applications within these folders.** Add applications and folders containing applications you want to allow. All applications in the subfolders of an allowed folder are also allowed. Unlike applications in the "Always allow these applications" list, applications listed here are not allowed if they or their paths are listed in the "Disallow applications within these folders" list.

If an application or its folder doesn't appear in these lists, the user can't open the application.

Some applications don't fully support signatures. To make sure a signed application is restricted, make a copy of the application, sign it, and move it to a location in the "Disallow applications within these folders" list. When you try to open the application on a managed computer, it should open because the signature is valid.

Next, void the signed application's signature by copying a file into its application package. Now when you try to open the application on a managed computer, it should not open because the signature is void and the application is in a disallowed folder.

To manage Applications preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Applications and then click the Applications tab.
5. Set the management setting to Always.
6. Select "Restrict which applications are allowed to launch."

7 Click the Applications tab (in the Applications pane), click the Add (+) button, choose an application you want to always allow, and then click Add.

When you allow an application, you also allow all helper applications included with that application. You can deselect helper applications to disallow them.

8 If you're asked to sign the application, click Sign; if you're asked to authenticate, authenticate as a local administrator.

To add the application to the list as an unsigned application, click Don't Sign.

When you sign the application, Workgroup Manager tries to embed the signature. If you don't have write access to the application, Workgroup Manager creates a detached signature.

9 Click the Folders tab, click the Add (+) button next to "Disallow applications within these folders," and then choose folders containing applications you want to prevent users from launching.

10 Click the Add (+) button next to the "Allow applications within these folders" field and choose folders containing applications you want to allow.

Disallowing folders takes precedence over allowing them. If you allow a folder that is a subfolder of a disallowed folder, the subfolder is still disallowed.

11 Click Apply Now.

Allowing Specific Dashboard Widgets

If your users have Leopard or later installed, you can prevent them from opening unapproved Dashboard widgets by creating a list of approved widgets (which can include widgets included with Leopard and third-party widgets). To approve third-party widgets, you must be able to access them from your server.

The Dashboard widgets included with Leopard Server can be trusted. However, users can install third-party Dashboard widgets without authenticating. To protect systems against unauthorized use, allow users to use only trusted third-party Dashboard widgets.

Note: Because code signing is not supported, it is possible for users to bypass restrictions to Dashboard widgets. Therefore, you should implement a mechanism to regularly check available Dashboard widgets to ensure policy compliance.

To allow specific Dashboard widgets:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Applications and then click Widgets.

5 Set the management setting to Always.

6 Select "Allow only the following Dashboard widgets to run."

7 To allow specific widgets, click the Add (+) button, select the widget's .wdgt file, and then click Add.

The widgets included with Leopard are in /Library/Widgets.

8 To prevent users from opening specific widgets, select the widget and click the Remove (–) button.

9 Click Apply Now.

Disabling Front Row

With Workgroup Manager, you can disable Front Row.

To disable Front Row:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Applications and then click Front Row.

5 Set the management setting to Always.

6 Deselect Allow Front Row.

7 Click Apply Now.

From the Command Line:

```
# Securing Client Configuration Management Services
# ================================================
# If the intended target is a client system, the target for the dscl
# commands should be "/LDAPv3/127.0.0.1". If the management target is the
# server itself, then the target should be ".".

# Disable Front Row
dscl /LDAPv3/127.0.0.1 mcxset  /Computers/$COMPUTER com.apple.frontrow
     PreventActivation always -bool 1
```

Allowing Legacy Users to Open Applications and Folders

To control user access to applications in Tiger or earlier, you:

- Provide access to a set of approved applications that users can open
- Prevent users from opening a set of unapproved applications

You can also set options to further control user access to applications.

When users have access to local volumes, they can access applications on the computer's local hard disk. If you don't want to allow this, you can disable local volume access.

Applications use helper applications for tasks they can't complete independently. For example, if a user tries to open a web link in a mail message, the mail application might need to open a web browser to display the webpage.

Disallowing helper applications improves security because an application can designate any other application as a helper application. However, you might want to include common helper applications in the approved applications list. This avoids problems such as users being unable to open and view mail content or attached files.

Occasionally, applications or the operating system might require the use of UNIX tools, such as QuickTime Image Converter. These tools can't be accessed directly, and generally operate in the background without the user's knowledge. If you disallow access to UNIX tools, some applications might not work.

Allowing UNIX tools enhances application compatibility and efficient operation, but can decrease security.

If you don't manage Applications settings for computers running Leopard or later, Legacy settings are used.

To set up a list of accessible applications:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Applications and then click Legacy.
5. Set the management setting to Always.
6. Select "User can only open these applications" or "User can open all applications except these."
7. Add items to and remove items from the list.

 To select multiple items, hold down the Command key.

8. To allow access to applications stored on the user's local hard disk, select "User can also open all applications on local volumes."
9. To allow helper applications, select "Allow approved applications to launch non-approved applications."
10. To allow use of UNIX tools, select "Allow UNIX tools to run."
11. Click Apply Now.

From the Command Line:

```
# Setting up a list of accessible applications
# -------------------------------------------
# Allow access to applications stored on the user's local hard disk
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess OpenItemsInternalDrive always -bool 1

# Allow helper applications
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess ApprovedAppLaunchesOthers always -bool 1

# Allow UNIX tools
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess AllowUnbundledApps always -bool 1
```

Managing Dock Preferences

You can customize the user's Dock to display specific applications. This helps you guide the user toward using specifically recommended applications.

You can also add documents and folders to the Dock. Adding specific, required network folders to the Dock helps prevent the user from navigating through your network hierarchy. This also helps prevent them from misusing the server.

To manage Dock preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Dock and then click Dock Display.
5. Set the management setting to Once or Always.
6. Drag the Dock Size slider to make the Dock smaller or larger.

7 If you want items in the Dock to be magnified when a user moves the pointer over them, select Magnification and then adjust the slider.

Magnification is useful if you have many items in the Dock.

8 From the "Position on screen" radio buttons, select whether to place the Dock on the left, right, or bottom of the desktop.

9 From the "Minimize using" pop-up menu, choose a minimizing effect.

10 If you don't want to use animated icons in the Dock when an application opens, deselect "Animate opening applications."

11 If you don't want the Dock to be visible all the time, select "Automatically hide and show the Dock."

When the user moves the pointer to the edge of the screen where the Dock is located, the Dock appears.

12 Click Apply Now.

From the Command Line:

```
# Managing Dock Preferences
# -------------------------
# Set Dock hiding
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide always -bool 1
```

Managing Energy Saver Preferences

Energy Saver preference settings help you save energy and battery power by managing wake, sleep, and restart timing for servers and client computers. You can only manage Energy Saver preferences for computer lists.

When client computers go to sleep, they become unmanaged. Do not enable sleep mode for client computers.

To manage Energy Saver preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select computers or computer groups.

4 Click Energy Saver and then click Desktop.

5. From the OS pop-up menu, choose Mac OS X and set the management setting to Always.
6. To adjust sleep settings, choose Sleep from the Settings pop-up menu and move the "Put the computer to sleep when it is inactive for" slider to Never.
7. From the OS pop-up menu, choose Leopard Server and set the management setting to Always.
8. From the Settings pop-up menu, choose Sleep and move the "Put the computer to sleep when it is inactive for" slider to Never.
9. Click Portable.
10. From the Power Source pop-up menu, choose Adapter and set the management setting to Always.
11. From the Settings pop-up menu, choose Sleep and move the "Put the computer to sleep when it is inactive for" slider to Never.
12. From the Power Source pop-up menu, choose Battery and set the management setting to Always.
13. From the Settings pop-up menu, choose Sleep and move the "Put the computer to sleep when it is inactive for" slider to Never.
14. Click Schedule.
15. From the OS pop-up menu, choose Mac OS X and set the management setting to Always.
16. Deselect "Start up the computer."
17. From the OS pop-up menu, choose Leopard Server and set the management setting to Always.
18. Deselect "Start up the computer."
19. Click Apply Now.

Managing Finder Preferences

You can control aspects of Finder menus and windows to improve or control workflow.

You can prevent users from burning media or from ejecting disks, and from connecting to remote servers. When used with Dock preferences, you can guide the user experience.

To manage Finder preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3. Select users, groups, computers, or computer groups.
4. Click Overview.
5. Click Finder, click the Preferences tab, and then select Always.
6. Select "Use normal Finder."

 Simple Finder is best used for computers in kiosk situations.

 Simple Finder removes the ability to use a Finder window to access applications or modify files. This limits users to accessing only what is in the Dock. If you enable Simple Finder, users cannot mount network volumes. With Simple Finder enabled, users cannot create folders or delete files.
7. Deselect "Hard disks," "Removable media (such as CDs)," and "Connected servers."

 By deselecting these, you help prevent users from casually navigating through local and network file systems.
8. Select "Always show file extensions."

 Important: Operating systems use file extensions as one method of identifying types of files and their associated applications. Using only file extensions to check the safety of incoming files leaves your system vulnerable to attacks by Trojans. A Trojan is a malicious application that uses common file extensions or icons to masquerade as a document or media file (such as a PDF, MP3, or JPEG).

 For further explanation and guidance on handling mail attachments and content downloaded from the internet, see KBase Article 108009: Safety tips for handling email attachments and content downloaded from the Internet at docs.info.apple.com/article.html?artnum=108009.
9. Click Commands and select Always.
10. Deselect Connect to Server, Go to iDisk, and Go to Folder.

 Instead of allowing the user to choose which servers or folders to load, add approved servers.
11. Deselect Eject and Burn Disc.

 Disallowing external media gives you more control.
12. Deselect Restart and Shut Down.

 By disallowing restarting and shutting down client computers, you help ensure that your computers are available to other users.
13. Click Apply Now.

From the Command Line:

```
# Managing Finder Preferences
# --------------------------
# Manage Finder preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     AppleShowAllExtensions-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitBurn always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitConnectTo always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitEject always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToFolder always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToiDisk always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowHardDrivesOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowMountedServersOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowRemovableMediaOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     AppleShowAllExtensions always -bool 1
```

Managing Login Preferences

Use Login preferences to set options for user login, to provide password hints, and to control the user's ability to restart and shut down the computer from the login window. You can also mount a group volume or set applications to open when a user logs in.

The table below summarizes what you can do with settings in each Login pane.

Login preference pane	What you can control
Window	*For computers and computer groups only:* The appearance of the login window such as the heading, message, which users are listed if the "List of users" is specified, and the ability to restart or shut down
Options	*For computers and computer groups only:* Login window options like enabling password hints, automatic login, console, fast user switching, inactivity logout, disabling of management, setting the computer name to match the computer record, and external account login
Access	*For computers and computer groups only:* Who can log in, if local users can use workgroup settings, and the combination and selection of workgroups

Login preference pane	What you can control
Scripts	*For computers and computer groups only:* A script to run during login or logout and whether to execute or disable the client computer's own LoginHook or LogoutHook scripts
Items	Access to the group volume, which applications open automatically for the user, and if users can add or remove login items

By managing script settings, you can help protect your users from malicious login or logout scripts that could be used to compromise their accounts integrity.

You can manage login window settings to make it more difficult for intruders to attempt to log in as legitimate users.

You can configure options to track malicious user actions.

To manage Login preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select user accounts.

 To perform the steps involving applying scripts and login window settings, select computers or computer groups.
4. Click Overview and click Login.
5. Click Items and select Always.

 Different login items settings are available depending on whether you're managing Once or Always. Like all managed preferences, you should use the Always setting to ensure that your settings stay in effect past the user's first login.
6. To load applications or to mount a group volume at startup, click Add to open a dialog where you can add an application or volume.
7. Add the applications required, including antivirus and file integrity checking applications required by your organization.
8. Deselect "Add network home share point."

 Instead of automatically mounting share points, the user should mount share points as required.
9. Deselect "User may add and remove additional items" and "User may press Shift to keep items from opening."

 Deselecting these options helps prevent the user from loading potentially malicious applications. It also helps ensure that the user cannot bypass loading applications required by your organization.

10 Click Scripts and select Always.

11 Unless your organization requires the use of specific login or logout scripts, deselect Login Script and Log-Out Script, and then deselect "Also execute the client computer's LoginHook script," and "Also execute the client computer's LogoutHook script."

To run login and logout scripts, the client's computer must have a level of trust with the server. This level of trust is based on how secure the client's connection is with the server. By requiring a level of trust, this ensures that the client computer does not run scripts from malicious servers.

For more information about how to enable the use of login and logout scripts, see the *User Management* guide.

12 Click Window and select Always.

13 Select "Login Window message" and enter help desk contact information in the adjacent field.

Do not enter information about the computer's typical usage or who its users are.

14 In "Display Login Window as," select "Name and password text fields."

Requiring that users know their account names adds a layer of security and helps prevent intruders from compromising accounts with weak passwords.

15 Deselect "Show Restart button in the Login Window" and "Show Shut Down button in the Login Window."

Preventing users from easily restarting or shutting down the computer helps ensure that the computer is available to all users.

16 Deselect "Show password hint after 3 attempts to enter a password."

Password hints can help malicious users compromise accounts. If you enable this setting, set the password hint per user account to information for your organization's help desk.

17 Deselect "Auto Login Client Setting."

Enabling this setting allows users to enable automatic login through System Preferences. Automatic login bypasses all login window-based security mechanisms.

18 Deselect "Allow users to log in using '>console.'"

Enabling this setting allows the user to bypass the login window and use the Darwin console (command-line interface).

19 Click Options and select Always.

20 Deselect Enable Fast User Switching.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is actively using the computer.

21 Deselect "Log out users after # minutes of inactivity."

If you select "Log out users after # minutes of inactivity," enable password-protected screensavers in case a dialog prevents logging out.

22 Click Apply Now.

From the Command Line:

```
# Managing Login Preferences
# -------------------------
# Manage Login preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     LoginwindowText always -string "$LOGIN WINDOW MESSAGE"
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     mcx_UseLoginWindowText always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     RestartDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     ShutDownDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     SHOWFULLNAME always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     DisableConsoleAccess always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     MultipleSessionEnabled always -bool 0
```

Managing Media Access Preferences

Media Access preferences let you control settings for, and access to, CDs, DVDs, the local hard disk, and external disks (for example, floppy disks and FireWire drives).

Disable unnecessary media. If users can access external media, it provides opportunities for performing malicious activities. For example, they can transfer malicious files from the media to the hard disk. Another example is if an intruder gains temporary access to the computer, he or she can quickly transfer confidential files to the media.

Carefully weigh the advantages and disadvantages of disabling media. For example, disabling external disks prevents you from using USB flash memory drives for storing keychains. For more information, see "Storing Credentials in Keychains" on page 107.

To manage Media Access preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Overview and click Media Access.
5. Select Always and click Disc Media.
6. Unless you must use disc media, deselect Allow for CDs & CD-ROMs, DVDs, and Recordable Discs.

 To enable disc media, select both Allow and Require Authentication for that disc media.
7. Click Other Media.
8. Unless you must use media, deselect Allow for Internal Disks and External Disks.

 If you must enable media, select Allow and Require Authentication for that disc media. Select Read-Only if you do not need to save files to that media.
9. Select "Eject all removable media at logout."

 This helps prevent users from forgetting they have media inserted in the computer.
10. Click Apply Now.

Managing Mobility Preferences

You can use Mobility preferences to enable and configure mobile accounts for users during their next login.

If your computers have Leopard or later, you can also encrypt the contents of the mobile account's portable home directory, restrict its size, choose its location, or set an expiration date on the account.

Mobile accounts include a network home folder and a local home folder. By having these two types of home folders, clients can take advantage of features available for local and network accounts. You can synchronize specific folders of these two home folders, creating a portable home directory.

Avoid using mobile accounts. When you access a mobile account from a client computer and create a portable home directory, you create a local home folder on that client computer. If you access the mobile account from many computers, creating portable home directories on each computer, your home folder's files are stored on several computers. This provides additional avenues of attack.

If you use mobile accounts, do not create portable home directories on computers that are physically insecure, or that you infrequently access. Enable FileVault on every computer where you create portable home directories. For more information about enabling FileVault, see "Securing Security Preferences" on page 138.

To manage Mobility preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select a user account, group account, computer, or computer group.
4. Click Overview.
5. Click Mobility, click Account Creation, and then click Creation.
6. Set the management setting to Always.
7. To disable mobile accounts, deselect "Create mobile account when user logs in to network account"; to enable mobile accounts, select this option.
8. Select "Require confirmation before creating a mobile account."

 If this is deselected, a portable home directory is created every time the user accesses a different computer.
9. Select "with syncing off."
10. Click Rules, click Login & Logout Sync, and select Always.
11. In the "Sync at login and logout" list, click the Add (+) button and enter the paths of folders located in the user's home folder.

 Alternatively, click the browse (…) button to open a dialog where you can choose folders to add to the list and then add folders that do not contain confidential files.
12. In the "Skip items that match any of the following" list, click the Add (+) button and enter the paths of folders located in the user's home folder.

 Alternatively, click the browse (…) button to open a dialog where you can choose folders to add to the list and then add folders that contain confidential files.
13. Deselect "Merge with user's settings."

 By deselecting this setting, the folders you choose to synchronize replace those chosen by the user.
14. Click Background Sync. Select Always.
15. In the "Sync at login and logout" list, click the Add (+) button and enter the paths of folders located in the user's home folder.

 Alternatively, click the browse (…) button to open a dialog where you can choose folders to add to the list and then add folders that do not contain confidential files.

16 In the "Skip items that match any of the following" list, click the Add (+) button and enter the paths of folders located in the user's home folder.

Alternatively, click the browse (…) button to open a dialog where you can choose folders to add to the list and then add folders that contain confidential files.

17 Deselect "Merge with user's settings."

By deselecting this setting, the folders you choose to synchronize replace those chosen by the user.

18 Click Apply Now.

Managing Network Preferences

Network preferences let you select and configure proxy servers that can be used by users and groups. You can also specify hosts and domains to bypass proxy settings.

Using proxy servers controlled by your organization can help improve security. You can also decrease the performance hit from using proxies if you selectively bypass trusted hosts and domains (like choosing local resources or trusted sites).

You can also disable Internet Sharing, AirPort, or Bluetooth. Disabling these can improve security by removing avenues for attack.

To manage Network preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Overview.

5 Click Network and then click Proxies.

6 Set the management setting to Always.

7 Select a type of proxy server and enter the network address and port of a proxy server controlled by your organization.

8 If you select Automatic Proxy Configuration, enter the URL of your automatic proxy configuration (.pac) file.

9 In the "Bypass proxy settings for these Hosts & Domains" field, enter the addresses of the hosts and domains that you want users to connect to directly.

To enter multiple address, separate the subnet masks with new lines, spaces, semicolons, or commas. There are several ways to enter addresses:

- A subdomain or fully qualified domain name (FQDN) of a target server, such as server1.apple.com or store.apple.com.
- The specific IP address of a server, such as 192.168.2.1.
- A domain name, such as apple.com. This bypasses apple.com, but not subdomains, such as store.apple.com.
- An website, including subdomains, such as *.apple.com.
- A subnet in Classless Inter-Domain Routing (CIDR) notation. For example, to add a subnet of IP addresses from 192.168.2.0 to 192.168.2.255, name that view 192.168.2.0/24. For a description of subnet masks and CIDR notation, see the *Network Services Administration* guide.

10 Deselect Use Passive FTP Mode (PASV).

11 Click Apply Now.

From the Command Line:

```
# Managing Network Preferences
# ----------------------------
# Manage Network preferences
networksetup -setwebproxystate Ethernet on
networksetup -setwebproxy Ethernet "http://$SERVER" 8008

networksetup -setpassiveftp Ethernet on
```

Managing Parental Controls Preferences

Parental Controls preferences allow you to hide profanity in Dictionary, limit access to websites, or set time limits or other constraints on computer usage. To manage Parental Controls preferences, computers must have Leopard or later.

Note: Parental control does not apply to directory users. It applies to only local users.

The table below describes what settings in each Parental Controls pane can do.

Parental Controls preference pane	What you can control
Content Filtering	Whether profanity is allowed in Dictionary, and limitations on which websites users can view
Time Limits	How long and when users can log in to their accounts

Hiding Profanity in Dictionary

You can hide profane terms from the Dictionary application included with Leopard or later. When you hide profane terms, entirely profane terms are removed from search results. If you search for a profane term that has an alternate nonprofane definition, Dictionary only displays the nonprofane definition.

To hide profanity in Dictionary:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Parental Controls and then click Content Filtering.
5. Set the management setting to Always.
6. Select "Hide profanity in Dictionary."
7. Click Apply Now.

From the Command Line:

```
# Managing Parental Control Preferences
# -------------------------------------
# Hide profanity
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.Dictionary
     parentalControl always -bool 1
```

Preventing Access to Adult Websites

You can use Workgroup Manager to help prevent users from visiting adult websites. You can also block access to specific websites while allowing users to access other websites. You can allow or deny access to specific subfolders in the same website.

Instead of preventing access to specific websites, you can allow access only to specific websites. For more information, see "Allowing Access Only to Specific Websites" on page 319.

To prevent access to websites:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.

4 Click Parental Controls and then click Content Filtering.

5 Set the management setting to Always.

6 Select "Limit access to websites by" and choose "trying to limit access to adult websites."

7 To allow access to specific sites, click the Add (+) button next to the "Always allow sites at these URLs" list and then enter the URL of the site you want to allow.

8 To block access to specific sites, click the Add (+) button next to the "Never allow sites at these URLs" list and then enter the URL of the site you want to block.

 To allow or block a site, including all content stored in its subfolders, enter the highest level URL of the site.

 For example, allowing http://www.example.com/ lets the user view all pages in www.example.com. However, blocking http://www.example.com/banned/ prevents the user from viewing content stored in www.example.com/banned/, including all subfolders in /banned/ but it allows the user to view pages in www.example.com that are not in /banned/.

9 Click Apply Now.

Allowing Access Only to Specific Websites

You can use Workgroup Manager to allow access only to specific websites on computers with Leopard or later.

If the user tries to visit a website that he or she is not allowed to access, the web browser loads a webpage that lists all sites the user is allowed to access.

To help direct users to allowed sites, the user's bookmarks are replaced by websites you allow access to. The bookmarks created by allowing access to websites are called *managed bookmarks*.

If the user syncs bookmarks with MobileMe, the first time the user syncs he or she is asked if MobileMe should merge or replace its bookmarks with the managed bookmarks. If the user merges bookmarks, the MobileMe bookmarks will include the original MobileMe bookmarks and the managed bookmarks. If the user replaces bookmarks, the MobileMe bookmarks include only the managed bookmarks.

You can also use Workgroup Manager to block specific websites instead of blocking all websites. For more information, see "Preventing Access to Adult Websites" on page 318.

To allow access only to specific websites:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Parental Controls and then click Content Filtering.

5 Set the management setting to Always.

6 Select "Limit access to websites by" and choose "allowing access to the following websites only."

7 Use one of the following methods to add websites that you want to allow access to:

- In Safari, open the site and then drag the icon from the address bar (of Safari) to the list.
- In Safari, choose Bookmarks > Show All Bookmarks, then drag icons from the bookmark list to the list in Workgroup Manager.
- If you have a .webloc file of the website you want to allow access to, drag the file into the list.
- If you don't have a .webloc file of the website you want to allow access to, click the Add (+) button and enter the URL of the website you want to allow.

 In the "Web site title" field, name the website. In the Address field, enter the highest level URL of the site.

 For example, allowing http://www.example.com/ lets the user view all pages in www.example.com. Allowing http://www.example.com/allowed/ lets the user view content stored in www.example.com/allowed/, including all subfolders in /allowed/, but not folders located outside of /allowed/.

8 To create folders to organize websites, click the New Folder (folder) button, then double-click the folder to rename it.

To add URLs within a folder, open the folder's disclosure triangle, select the folder, and then click the Add (+) button.

To create a subfolder, open a folder's disclosure triangle, select the folder, and then click the New Folder (folder) button.

9 To change the name or URL of a website, double-click the website entry; then, to rename a folder, double-click the folder entry.

10 To rearrange websites or folders, drag the websites or folders in the list.

11 Click Apply Now.

Setting Time Limits and Curfews on Computer Usage

You can use Workgroup Manager to set time limits and curfews for computer usage on computers with Leopard or later.

If you set a time limit for computer usage, users who meet their daily time limits can't log in until the next day when their quota is reset. You can set different time limits for weekdays (Monday through Friday) and weekends (Saturday and Sunday). The time limit can range from 30 minutes to 8 hours.

If you set a curfew, users can't log in during the days and times you specify. If a user is logged in when their curfew starts, the user is immediately logged out. You can set different times for weekdays (denying access Sunday nights through Thursday nights) and weekends (Friday and Saturday nights).

To set time limits and curfews:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Parental Controls and then click Time Limits.
5. Set the management setting to Always and then select "Enforce limits."
6. To set time limits, click Allowances, then under Weekdays or Weekends select "Limit computer use to" and drag the slider to amount of time you want to limit use.
7. To set curfews, click Curfews, select "Sunday through Thursday" or "Friday and Saturday," and then enter the range of time when you want to prevent computer access.

 You can highlight the time and replace it with a new time, or you can highlight the time and click the up or down buttons next to the time.
8. Click Apply Now.

Managing Printing Preferences

Printer preferences let you control which printers the user can access. Ideally, reduce the printer list to only those printers the user needs to access.

You should require that the user authenticate as an administrator before printing.

To manage Printing preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

 To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select users, groups, computers, or computer groups.
4. Click Printing and then click Printers.
5. Set the management setting to Always.
6. Click Printer List.

7 In the Available Printers list select a printer and click Add.

Add printers that you want the user to access to the user's printer list.

8 If you want to add additional printers to the user's printer list, click Open Printer Setup.

For more information, see Printer Setup Utility Help.

9 Deselect "Allow user to modify the printer list."

10 Deselect "Allow printers that connect directly to user's computer."

If you select this setting, select "Require an administrator password."

11 Click Access.

12 Select a printer, and select "Require an administrator password."

Repeat for all printers in the User's Printer List.

13 Click Apply Now.

From the Command Line:

```
# Managing Printing Preferences
# ----------------------------
# Manage Printing preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     RequireAdminToAddPrinters always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     AllowLocalPrinters always -bool 0
```

Managing Software Update Preferences

With Leopard Server, you can create your own Software Update server to control updates that are applied to specific users or groups. This is helpful because it reduces external network traffic while also providing more control to server administrators.

By configuring a Software Update server, server administrators can choose which updates to provide.

To manage Software Update preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Software Update.

5 Set the management setting to Always.

6 Specify a URL in the form http://someserver.apple.com:8088/index.sucatalog.

7 Click Apply Now.

From the Command Line:

```
# Managing Software Update Preferences
# -----------------------------------
# Manage Software Update preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.SoftwareUpdate
     CatalogURL always -string "http:/$SERVER:8088/index.sucatalog"
```

Managing Access to System Preferences

You can specify which preferences to show in System Preferences. If a user can see a preference, it does not mean the user can modify that preference. Some preferences, such as Startup Disk preferences, require an administrator name and password before a user can modify its settings.

The preferences that appear in Workgroup Manager are those installed on the computer you're using. If your administrator computer is missing preferences that you want to disable on client computers, install the applications related to those preferences or use Workgroup Manager on a computer that includes those preferences.

To manage System Preferences preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click System Preferences.

5 Set the management setting to Always.

6 Click Show None.

7 Select the following items to show in System Preferences:

- Appearance
- Select Displays
- Select Dock
- Select Expose & Spaces
- Select Keyboard & Mouse
- Select Security
- Select Universal Access

8 Click Apply Now.

Managing Universal Access Preferences

Universal Access settings can help improve the user experience for some users. For example, if a user has difficulty using a computer or wants to work in a different way, you can choose settings that enable the user to work more effectively.

Most Universal Access settings do not negatively impact security. However, some settings allow other users to more easily see what you're doing.

To manage Universal Access preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select users, groups, computers, or computer groups.

4 Click Universal Access.

5 Click Seeing and then set the management setting to Always.

6 Deselect Turn on Zoom.

Pressing and holding the Option, Command, and + keys will zoom in, while pressing and holding the Option, Command, and - keys will zoom out.

7 Click Keyboard and select Always.

8 Select Sticky Keys Off and deselect "Show pressed keys on screen."

If Sticky Keys are on and you select "Show pressed keys on screen," modifier keys such as Control, Option, Command, and Shift are displayed on screen. All other keys are not displayed.

9 Click Apply Now.

From the Command Line:

```
# Managing Universal Access Preferences
# -------------------------------------
# Manage Universal Access preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKey always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyBeepOnModifier always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyShowWindow always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewDriver always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewShowPreview always -bool 0
```

Enforcing Policy

When you implement a policy for controlling the user experience by removing certain files (from example, Kernel extensions) or managing user-controllable settings (for example, screen saver settings), you should also implement a mechanism for reenforcing the policy in case the deleted files are restored or the settings are changed by users or by software updates.

Using `mcx`, `cron`, or `launchd` jobs, create scripts that run during startup and shutdown and after software updates to reenforce policy in case of violations.

To protect the policy enforcements scripts, compile them into binary format so that users can't modify them.

Securing NetBoot Service

22

Use this chapter to learn how to secure NetBoot service.

Securely configuring client configuration management through NetBoot helps standardize the clients across your network and provides a secure deployment.

Network computers can be managed through NetBoot, which decreases maintenance time and can help prevent malicious software attacks.

Securing NetBoot Service

By using NetBoot you can have your client computers start up from a standardized Leopard configuration suited to their specific tasks. Because the client computers start up from the same image, you can quickly update the operating system for an entire group by updating a single boot image.

A *boot image* is a file that looks and acts like a mountable disk or volume. NetBoot images contain the system software needed to act as a startup disk for client computers over the network.

An *installation image* is an image that starts up the client computer long enough to install software from the image. The client can then start up from its own hard drive.

Boot images (NetBoot) and installation images (NetInstall) are different kinds of disk images. The main difference is that a .dmg file is a proper disk image and a .nbi folder is a bootable network volume (which contains a .dmg disk image file). Disk images are files that behave like disk volumes.

For more information about configuring NetBoot service, see the *System Imaging and Software Update Administration* guide.

Disabling NetBoot Service

If your server is not intended to be a NetBoot server, disable the NetBoot service. Disabling the service prevents potential vulnerabilities on your computer. The NetBoot service is disabled by default, but verification is recommended.

The best way to prevent clients from using NetBoot on the server is to disable NetBoot service on all Ethernet ports.

To disable NetBoot:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click NetBoot.
4. Click General.
5. Disable NetBoot on all ports.
6. Click Stop NetBoot (below the Servers list).

From the Command Line:

```
# ------------------------------------------------------------------
# Securing NetBoot Service
# ------------------------------------------------------------------

# Disable NetBoot
serveradmin stop netboot
```

Securely Configuring NetBoot Service

If NetBoot service is required, it should be provided over a trusted network.

Securely configure NetBoot service with restrictions on the ports it uses, the images available, and client access to the service. NetBoot service uses Apple Filing Protocol (AFP), Network File System (NFS), Dynamic Host Configuration Protocol (DHCP), Web, and Trivial File Transfer Protocol (TFTP) services, depending on the types of clients your are trying to boot. You must also securely configure services to reduce network vulnerabilities.

NetBoot service creates share points for storing NetBoot and NetInstall images in /Library/NetBoot/ on each volume you enable and names them NetBootSP*n*, where *n* is 0 for the first share point and increases by 1 for each extra share point.

For example, if you decide to store images on three server disks, NetBoot service sets up three share points named NetBootSP0, NetBootSP1, and NetBootSP2.

You can restrict access to NetBoot service on a case-by-case basis by listing the hardware addresses (also known as the Ethernet or MAC addresses) of computers that you want to permit or deny access to.

The hardware address of a client computer is added to the NetBoot Filtering list when the client starts up using NetBoot and is, by default, enabled to use NetBoot service. You can specify other services.

To securely configure NetBoot:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select NetBoot.
4. Click Settings, then click Filters.

 NetBoot service filtering lets you restrict access to the service based on the client's Ethernet hardware (MAC) address. A client's address is added to the filter list the first time it starts up from an image on the server and is allowed access by default.
5. Select "Enable NetBoot/DHCP filtering."
6. Select "Allow only clients listed below (deny others)" or "Deny only clients listed below (allow others)."
7. Use the Add (+) button to enter the canonical or noncanonical form of a hardware address to the filter list, or use the Delete (–) button to remove a MAC address from the filter list.

 To look up a MAC address, enter the client's DNS name or IP address in the Host Name field and click Search.

 To find the hardware address for a computer using Leopard, look on the TCP/IP pane of the computer's Network preference or run Apple System Profiler.
8. Click OK.
9. Click Save.

Note: You can also restrict access to a NetBoot image by selecting the name of the image in the Images pane of the NetBoot service settings in Server Admin, clicking the Edit (/) button, and providing the required information.

From the Command Line:

```
# Securely configure NetBoot
defaults rename /etc/bootpd allow_disabled allow
```

Viewing NetBoot Service Logs

NetBoot service logging is important to security. With logs, you can monitor and track client communication to the NetBoot server. The NetBoot service log is /var/log/system.log that can be accessed using Server Admin.

To view NetBoot service logs:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click NetBoot.
4. Click Logs to display the contents of system.log.

From the Command Line:

```
# View NetBoot service logs
tail /var/log/system.log | grep bootpd
```

Securing Software Update Service 23

Use this chapter to learn how to secure Software Update service.

You can protect against attacks by configuring an internal Software Update server. This allows you to maintain a secure network by controlling what software updates are installed on your network computers.

Disabling Software Update Service

If your server is not intended to be a software update server, disable the Software Update service. Disabling the service prevents potential vulnerabilities on your computer. Software Update service is disabled by default, but verification is recommended.

To disable Software Update:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect Software Update.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Software Update Service
# ------------------------------------------------------------------

# Disable Software Update
serveradmin stop swupdate
```

Securely Configuring Software Update Service

Software Update service offers you ways to manage Macintosh software updates from Apple on your network. In an uncontrolled environment, users might connect to Apple Software Update servers at any time and update client computers with software that is not approved by your IT group.

By using local Software Update servers, your client computers access only the software updates you permit from software lists that you control, giving you more flexibility in managing computer software updates.

You can restrict client access in a Software Update server by disabling automatic mirror-and-enable functions in the General Settings pane. You manage specific updates in the Updates pane of the Software Update server.

To specify which client can access software updates:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Software Update.
4. Click Settings, then click General.
5. To immediately disable all software updates for client users, deselect "Automatically enable copied updates."
6. Click Updates.
7. Click Update List to refresh the list of available software updates.

 This list provides the date the update was posted and the name, version number, and size of the update.
8. Click Copy Now to copy software updates to your server.

 This copies software updates to your server.
9. In the Enable column, select the checkbox for each update you want to make available to client computers.

10 Click Save.

From the Command Line:

```
# Specify which client can access software updates
serveradmin settings swupdate:autoEnable = no
```

Viewing Software Update Service Logs

Software Update service logging is important for security. With logs, you can monitor and track communication through the Software Update service. Access the Software Update service log, /var/log/system.log, using Server Admin.

To view Software Update service logs:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click Software Update.

4 Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View Software Update service logs
tail /var/log/swupd/swupd_*
```

Securing Directory Services

24

Use this chapter to learn how to secure Directory service.

Directory services are the backbone of your network's security policy. The granting of access to the information and services on your network should be well-planned and thought out.

A directory service provides a central repository for information about computer users and network resources in an organization. Leopard Server uses Open Directory for its directory service.

The directory services provided by Leopard Server use LDAPv3, as do many other servers. LDAPv3 is an open standard common in mixed networks of Macintosh, UNIX, and Windows systems. Some servers use the older version, LDAPv2, to provide directory service.

Open Directory also provides authentication service. It can securely store and validate the passwords of users who want to log in to client computers on your network or use other network resources that require authentication. Open Directory can also enforce policies such as password expiration and minimum length.

For more information about passwords and authentication, see Appendix A, "Understanding Passwords and Authentication," on page 394.

Open Directory must be set to the proper role and configured to use SSL to encrypt its communications to protect the confidentiality of its important authentication data. Password policies can also be enforced by Open Directory.

For more information about understanding and configuring directory and authentication services, see the *Open Directory Administration* guide.

Open Directory Server Roles

Open Directory can be configured to one of several roles, depending on the server's place in the network and directory structure:

- Standalone Server—This role does not share information with other computers on the network. It is a local directory domain only.
- Connected to a Directory Server—This role allows the server to get directory and authentication information from another server's shared directory domain.
- Open Directory Master—This role provides an Open Directory Password Server, which supports conventional authentication methods required by Leopard Server services. In addition, an Open Directory Master can provide Kerberos authentication for single sign-on.
- Open Directory Replica—This role acts as a backup to the Open Directory master. It can provide the same directory and authentication information to other networks as the master. It has a read-only copy of the master's LDAP directory domain.

Configuring the Open Directory Services Role

If the server is not intended to be a directory server, make sure the LDAP server is stopped using Server Admin. To stop LDAP server, set the Open Directory role to Standalone Server. This prevents Open Directory from engaging in unnecessary network communications.

On a newly installed server, the LDAP server should be stopped by default, but verification is recommended.

To configure the Open Directory role:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Open Directory.
4. Click Settings, then click General.
5. Click Change.

 The Service Configuration Assistant opens.
6. Choose a role, then click Continue.
7. Confirm the Open Directory configuration settings, then click Continue.
8. If the server was an Open Directory master and you are sure that users and services no longer need access to the directory data stored in the shared directory domain that the server has been hosting, click Close.

9 Click the Open Directory Utility button to configure access to directory systems.

If you connect Tiger Server or later to a directory domain of Mac OS X Server v10.3 or earlier, users defined in the older directory domain cannot be authenticated with the NTLMv2 method. This method might be required to securely authenticate some Windows users for the Windows services of Server Tiger or later.

Open Directory Password Server in Tiger Server or later supports NTLMv2 authentication, but Password Server in Mac OS X Server v10.3 or earlier does not support NTLMv2.

Similarly, if you configure Tiger Server or later to access a directory domain of Mac OS X Server v10.2 or earlier, users defined in the older directory domain cannot be authenticated with the MS-CHAPv2 method. This method might be required to securely authenticate users for the VPN service of Tiger Server or later.

Open Directory in Tiger Server supports MS-CHAPv2 authentication, but Password Server in Mac OS X Server v10.2 does not support MS-CHAPv2.

10 If the server you're configuring has access to a directory system that also hosts a Kerberos realm, you can join the server to the Kerberos realm.

To join the Kerberos realm, you need the name and password of a Kerberos administrator or a user who has the authority to join the realm.

11 Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Directory Services
# ------------------------------------------------------------------

# Configure the Open Directory role
slapconfig -createldapmasterandadmin $ADMIN $ADMIN_FULL_NAME $ADMIN_UID
     $SEARCH_BASE $REALM
```

Starting Kerberos After Setting Up an Open Directory Master

If Kerberos doesn't start when you set up an Open Directory master, you can use Server Admin to start it manually, but first you must fix the problem that prevented Kerberos from starting. Usually the problem is that the DNS service isn't correctly configured or isn't running.

Note: After you manually start Kerberos, users whose accounts have Open Directory passwords and were created in the Open Directory master's LDAP directory while Kerberos was stopped might need to reset their passwords the next time they log in. A user account is therefore affected only if all recoverable authentication methods for Open Directory passwords were disabled while Kerberos was stopped.

To start Kerberos manually on an Open Directory master:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Open Directory.
4. Click Refresh (or choose View > Refresh) and verify the status of Kerberos as reported in the Overview pane.

 If Kerberos is running, there's nothing more to do.
5. Verify that the DNS name and address resolve correctly by using Network Utility (in /Applications/Utilities/) to do a DNS lookup of the Open Directory master's DNS name and a reverse lookup of the IP address.

 If the server's DNS name or IP address doesn't resolve correctly:

 - In the Network pane of System Preferences, look at the TCP/IP settings for the server's primary network interface (usually built-in Ethernet). Make sure the first DNS server listed is the one that resolves the Open Directory server's name.
 - Check the configuration of DNS service and make sure it's running.
6. In Server Admin, select Open Directory for the master server, click Settings, then click General.
7. Click Kerberize, then enter the following information:

 - *Administrator Name* and *Password:* You must authenticate as an administrator of the Open Directory master's LDAP directory.
 - *Realm Name:* This field is preset to be the same as the server's DNS name converted to capital letters. This is the convention for naming a Kerberos realm. If necessary, you can enter a different name.

From the Command Line:

```
# Start Kerberos manually on an Open Directory master
kdcsetup -a $ADMIN $REALM
```

Configuring Open Directory for SSL

Using Server Admin, you can enable Secure Sockets Layer (SSL) for encrypted communications between an Open Directory server's LDAP directory domain and computers that access it.

SSL uses a digital certificate to provide a certified identity for the server. You can use a self-signed certificate or a certificate obtained from a Certificate Authority (CA).

SSL communications for LDAP use port 636. If SSL is disabled for LDAP service, communications are sent as clear text on port 389.

To set up SSL communications for LDAP service:

1. Open Server Admin and connect to the Open Directory master or an Open Directory replica server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Open Directory.
4. Click Settings, then click LDAP.
5. From the Configure pop-up menu, choose LDAP Settings, then select Enable SSL.
6. Use the Certificate pop-up menu to choose an SSL certificate that you want LDAP service to use.

 The menu lists all SSL certificates installed on the server. To use a certificate not listed, choose Custom Configuration from the pop-up menu.
7. Click Save.

From the Command Line:

The following steps describe the command-line method for creating certificates. For information about defining, obtaining, and installing certificates on your server using Certificate Manager in Server Admin, see "Obtaining Certificates" on page 191.

To create an Open Directory service certificate:

1. Generate a private key for the server in the /usr/share/certs/ folder:

 If the /usr/share/certs folder does not exist create it.

   ```
   $ sudo openssl genrsa -out ldapserver.key 2048
   ```
2. Generate a CSR for the CA to sign:

   ```
   $ sudo openssl req -new -key ldapserver.key -out ldapserver.csr
   ```

3. Fill out the following fields as completely as possible, making certain that the Common Name field matches the domain name of the LDAP server exactly:

```
Country Name:
Organizational Unit:
State or Province Name:
Common Name:
Locality Name (city):
Email Address:
Organization Name:
```

Leave the challenge password and optional company name blank.

4. Sign the ldapserver.csr request with the `openssl` command.

```
$ sudo openssl ca -in ldapserver.csr -out ldapserver.crt
```

5. When prompted, enter the CA passphrase to continue and complete the process.

 The certificate files needed to enable SSL on the LDAP server are now in the /usr/share/certs/ folder.

6. Open Server Admin.
7. In the Computers & Services list, select Open Directory for the server that is an Open Directory master or an Open Directory replica.
8. Click Settings.
9. Click Protocols.
10. From the Configure pop-up menu, choose "LDAP Settings."
11. Select Enable Secure Sockets Layer (SSL).
12. Use the Certificate pop-up menu to choose an SSL certificate that you want LDAP service to use.

 The menu lists SSL certificates that have been installed on the server. To use a certificate not listed, choose Custom Configuration from the pop-up menu.

13. Click Save.

Configuring Open Directory Policies

You can set password, binding, and security policies for an Open Directory master and its replicas. You can also can set several LDAP options for an Open Directory master or replica.

For more information about configuring policies, see "Configuring User Accounts" on page 185.

Setting the Global Password Policy

Using Server Admin, you can set a global password policy for user accounts in a Leopard Server directory domain.

The global password policy affects user accounts in the server's local directory domain. If the server is an Open Directory master or replica, the global password policy also affects user accounts that have an Open Directory password type in the server's LDAP directory domain.

If you change the global password policy on an Open Directory replica, the policy settings become synchronized with the master and replicas.

Administrator accounts are exempt from password policies. Each user can have a password policy that overrides global password policy settings. For more information, see "Password Policies" on page 401.

Kerberos and Open Directory Password Server maintain password policies separately. Leopard Server synchronizes the Kerberos password policy rules with Open Directory Password Server password policy rules.

To change the global password policy of user accounts in the same domain:

1. Open Server Admin and connect to an Open Directory master or replica server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Open Directory.
4. Click Settings, then click Policy.
5. Click Passwords.

 This allows you to set password policy options you want enforced for users who do not have individual password policies.
6. Select "differ from account name."
7. Select "contain at least one letter."
8. Select "contain at least one numeric character."
9. Select "be reset on first user login."
10. Select "contain at least 12 characters."
11. Select "differ from last 3 passwords used."

12 Select "be reset every 3 months."

Note: If you select an option that requires resetting the password, remember that some service protocols don't permit users to change passwords. For example, users can't change their passwords when authenticating for IMAP mail service.

13 Click Save.

Replicas of the Open Directory master automatically inherit its global password policy.

From the Command Line:

```
# Change the global password policy of user accounts in the same domain
pwpolicy -a $ADMIN_USER -setglobalpolicy "minChars=4
     maxFailedLoginAttempts=3"
```

From the Command Line

You can also set password policies by using the `pwpolicy` command in Terminal. For more information, see the Open Directory chapter of *Command-Line Administration*.

Setting a Binding Policy for an Open Directory Master and Replicas

Using Server Admin, you can configure an Open Directory master to permit or require trusted binding between the LDAP directory and the computers that access it. Replicas of an Open Directory master automatically inherit the master's binding policy.

Trusted LDAP binding is mutually authenticated. The computer proves its identity by using an LDAP directory administrator's name and password to authenticate to the LDAP directory. The LDAP directory proves its authenticity by means of an authenticated computer record created in the directory when you set up trusted binding.

Clients can't be configured to use trusted LDAP binding and a DHCP-supplied LDAP server (also known as DHCP option 95). Trusted LDAP binding is inherently a static binding, but DHCP-supplied LDAP is a dynamic binding.

Note: To use trusted LDAP binding, clients need Tiger or Tiger Server or later. Clients using Mac OS X v10.3 or earlier can't set up trusted binding.

To set the binding policy for an Open Directory master:

1 Open Server Admin and connect to the Open Directory master server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select Open Directory.

4 Click Settings, then click Policy.

5 Click Binding, then set the directory binding options you want:

- To *permit* trusted binding, select "Enable authenticated directory binding."
- To *require* trusted binding, also select "Require authenticated binding between directory and clients."

6 Click Save.

Important: If you enable "Encrypt all packets (requires SSL or Kerberos)" and "Enable authenticated directory binding," make sure your users are using only one for binding and not both.

From the Command Line:

```
# Set the binding policy for an Open Directory master
slapconfig -setmacosxodpolicy -binding required
```

Setting a Security Policy for an Open Directory Master and Replicas

Using Server Admin, you can configure a security policy for access to the LDAP directory of an Open Directory master.

Replicas of the Open Directory master automatically inherit the master's security policy.

Note: If you change the security policy for the LDAP directory of an Open Directory master, you must disconnect and reconnect (unbind and rebind) every computer connected (bound) to this LDAP directory using Directory Utility.

To set the security policy for an Open Directory master:

1 Open Server Admin and connect to the Open Directory master server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select Open Directory.

4 Click Settings, then click Policy.

5 Click Binding, then set the security options you want:

- "**Disable clear text passwords**" determines whether clients can send passwords as clear text if the passwords can't be validated using any authentication method that sends an encrypted password.
- "**Digitally sign all packets (requires Kerberos)**" certifies that directory data from the LDAP server won't be intercepted and modified by another computer while en route to client computers.
- "**Encrypt all packets (requires SSL or Kerberos)**" requires the LDAP server to encrypt directory data using SSL or Kerberos before sending it to client computers.

- "**Block man-in-the-middle attacks (requires Kerberos)**" protects against a rogue server posing as the LDAP server. Best if used with the "Digitally sign all packets" option.
- "**Disable client-side caching**" prevents client computers from caching LDAP data locally.
- "**Allow users to edit their own contact information**" permits users to change contact information on the LDAP server.

6 Click Save.

From the Command Line:

```
# Set the security policy for an Open Directory master
slapconfig -setmacosxodpolicy -cleartext blocked
```

Securing RADIUS Service

25

Use this chapter to learn how to secure RADIUS service.

By configuring a Remote Authentication Dial In User Service (RADIUS) server with Open Directory you can secure your wireless environment from unauthorized users.

Wireless networking gives companies greater network flexibility, seamlessly connecting laptop users to the network and giving them the freedom to move within the company while staying connected to the network.

This chapter describes how to configure and use RADIUS to keep your wireless network secure and to make sure it is used only by authorized users.

Disabling RADIUS Service

If your server is not intended to be a RADIUS server, disable RADIUS service. Disabling the service prevents potential vulnerabilities on your computer. RADIUS service is disabled by default, but verification is recommended.

To disable RADIUS service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect RADIUS.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Securing RADIUS Service
# ------------------------------------------------------------------

# Disable RADIUS service
radiusconfig stop
```

Securely Configuring RADIUS Service

RADIUS is used to authorize Open Directory users and groups so they can access AirPort Base Stations on a network. By configuring RADIUS and Open Directory you can control who has access to your wireless network.

RADIUS works with Open Directory and Password Server to grant authorized users access to the network through an AirPort Base Station. When a user attempts to access an AirPort Base Station, AirPort communicates with the RADIUS server using Extensible Authentication Protocol (EAP) to authenticate and authorize the user.

Users are given access to the network if their user credentials are valid and they are authorized to use the AirPort Base Station. If a user is not authorized, he or she cannot access the network through the AirPort Base Station.

Configuring RADIUS to Use Certificates

To increases the security and manageability of AirPort Base Stations, use Server Admin to configure RADIUS to use custom certificates. Using a certificate increases the security and manageability of AirPort Base Stations.

To use a custom certificate:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select RADIUS.
4. Click Settings.
5. From the RADIUS Certificate pop-up menu, choose a certificate.

 If you have a custom certificate, choose Custom Configuration from the Certificate pop-up menu and enter the path to the certificate file, private key file, and certificate authority file. If the private key is encrypted, enter the private key passphrase and click OK.

 If you don't have a certificate and want to create one, click Manage Certificates. For more information about creating certificates, see *Server Administration*.

6 Click Save.

From the Command Line:

```
# Use a custom certificate
serveradmin settings radius:eap.conf:CA_file = "/etc/certificates/$CA_CRT"
serveradmin settings radius:eap.conf:private_key_file =
     "/etc/certificates/$KEY"
serveradmin settings radius:eap.conf:private_key_password = "$PASS"
serveradmin settings radius:eap.conf:certificate_file =
     "/etc/certificates/$CERT"
```

Editing RADIUS Access

You can restrict access to the RADIUS service by creating a group of users and adding them to the service access control list (SACL) of RADIUS.

To edit RADIUS access:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select RADIUS.

4 Click Settings, then click Edit Allowed Users.

5 Select "For selected services below," then select RADIUS.

6 Select "Allow only users and groups below."

7 Click the Add (+) button.

8 From the Users and Groups list, drag users or groups of users to the "Allow only users and groups below" list.

If you want to remove users from the "Allow only users and groups below" list, select the users or groups of users and click the Delete (-) button. The user's in this list are the only ones who can use the RADIUS service.

From the Command Line:

```
# Edit RADIUS access
dseditgroup -o edit -a $USER -t user com.apple.access_radius
```

Viewing RADIUS Service Logs

Radius service logging is important for security. With logs, you can monitor and track communication through the Radius service. You can access the Radius service log, /var/log/system.log, using Server Admin.

To view the Radius service log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click Radius.
4. Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the Radius service log
tail /var/log/radius/radius.log
```

Securing Print Service

26

Use this chapter to learn how to secure Print service.

Print service is often an overlooked part of a security configuration. Important information passes into your networked printers so it is important that your printers are not misused.

With a print server, you can share printers by setting up print queues accessible by any number of users over a network connection. When a user prints to a shared queue, the print job waits on the server until the printer is available or until established scheduling criteria are met.

Apple's printing infrastructure is built on Common UNIX Printing System (CUPS). CUPS uses open standards such as Internet Printing Protocol (IPP) and PostScript Printer Description files (PPDs).

For more information about configuring print service, see the *Print Service Administration* guide.

Disabling Print Service

If your server is not intended to be a print server, disable the print server software. Disabling the service prevents potential vulnerabilities on your computer. Print service is disabled by default, but verification is recommended.

To disable Print service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click Print.
4. Click Stop Print (below the Servers list).

From the Command Line:

```
# ----------------------------------------------------------------------
# Securing Print Service
# ----------------------------------------------------------------------

# Disable Print service
serveradmin stop print
```

Securing Print Service

To increase security of your print service, configure service access controls and Kerberos.

Configuring Print Service Access Control Lists

You can configure Service Access Control Lists (SACLs) using Server Admin. SACLs enable you to specify which administrators have access to Print service.

SACLs provide you with greater control over which administrators have access to monitor and manage a service. The users and groups listed in a service's SACL are the only ones who can access the service. For example, to give administrator access to users or groups for the Print service on your server, add them to the Print service SACL.

To set administrator SACL permissions for Print service:

1. Open Server Admin and connect to the server.
2. Click Settings, then click Access.
3. Click Administrators.
4. Select the level of restriction that you want for the services.

 To restrict access to all services, select "For all services."

 To set access permissions for individual services, select "For selected services below" and then select Print service from the Service list.
5. To open the Users and Groups list, click the Add (+) button.
6. Drag users and groups from Users and Groups to the list.
7. Set the user's permission.

 To grant administrator access, choose Administrator from the Permission pop-up menu next to the user name.

 To grant monitoring access, choose Monitor from the Permission pop-up menu next to the user name.
8. Click Save.

From the Command Line:

```
# Set administrator SACL permissions for Print service
dseditgroup -o edit -a $USER -t user com.apple.monitor_print
```

Configuring Kerberos

You can configure Kerberos support for Print service IPP shared queues using CUPS v1.3 online web tools. The Print service then uses the local Kerberos server to authorize clients to print.

For your client computers to use Kerberos with Print service, the clients must be part of the same Kerberos realm. For information on how to join your client computers to a Kerberos realm, see *Open Directory Administration*.

In addition to joining the Kerberos realm, client computers must also use CUPS online web tools to configure Kerberos settings. The steps for configuring CUPS are the same on the client and server computers.

To configure Kerberos for Print service:

1. Open Safari browser.
2. Navigate to the CUPS online web administration tool at http://localhost:631.
3. Click the Administration tab.
4. Under Basic Server Settings, select the "Use Kerberos Authentication" checkbox.
5. Click Change Settings and authenticate if prompted.

 Print service is restarted and Kerberos is enabled.

 You can also edit the configuration file in CUPS by clicking Edit Configuration File in the Administration tab to open the /etc/cups/cupsd.conf file. Change the default authentication type from Basic to Negotiate, as shown:

   ```
   # Default authentication type, when authentication is required…
   DefaultAuthType Negotiate
   ```

From the Command Line:

```
# Configure Kerberos for Print service
cp /etc/cups/cupsd.conf $TEMP_FILE
/usr/bin/sed "/^DefaultAuthType.*/s//DefaultAuthType Negotiate/g"
     $TEMP_FILE > /etc/cups/cupsd.conf
```

Configuring Print Queues

If Print service is required, you should create a print queue for shared printers that is accessible by users over a network connection.

AppleTalk and Line Printer Remote (LPR) printer queues do not support authentication. Print service relies on the client to provide user information. Although standard Macintosh and Windows clients provide correct information, a clever user could potentially modify the client to submit false information and thereby avoid print quotas.

SMB service supports authentication, requiring users to log in before using SMB printers. Print service uses Basic and Digest (MD5) authentication and supports the IPP print job submission method.

You can share any printer that is set up in a print queue on the server. You create print queues using Server Admin.

To create a print queue:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click Print.
4. Click Queues.
5. Click the Add (+) button to add a print queue for a specific printer, and provide the following printer information for the printer the queue is created for:

 From the pop-up menu, choose the protocol used by the printer.

 For an AppleTalk printer, select the printer in the list and click OK.

 For an LPR printer, enter the printer IP address or DNS name and click OK.

 For an Open Directory printer, select the printer in the list and click OK.

 Enter the Internet address or DNS name for the printer.

 If you don't want to use the printer's default queue, deselect "Use default queue on server," enter a queue name, and click OK.
6. Select the queue you have added to the queue list.

 To verify that you have selected the correct queue, make sure the queue name matches the name next to Printer.

 Note: Changing the Sharing Name also changes the queue name that appears in Print & Fax preferences on the server.

7 In the Sharing Name field, enter the queue name you want clients to see.

Make sure the name is compatible with naming restrictions imposed by your clients. For example, some LPR clients do not support names that contain spaces, and some Windows clients restrict names to 12 characters. Queue names shared using LPR or SMB must not contain characters other than A–Z, a–z, 0–9, and _ (underscore).

AppleTalk queue names cannot be longer than 32 bytes. This might be fewer than 32 typed characters. The queue name is encoded according to the language used on the server and might not be readable on client computers using another language.

8 Select the printing protocols your clients use.

If you select "SMB," make sure you start SMB service.

9 If you want to enforce the print quotas you establish for users in Workgroup Manager, select the "Enforce quotas for this queue" checkbox.

10 If you want the printer to create a cover sheet, choose the title of the cover sheet from the Cover Sheet pop-up menu; otherwise, choose "None."

11 Click Save.

Viewing Print Service and Queue Logs

Print service keeps two types of logs: a print service log and individual print queue logs.

- The print service log records the time of events such as when print service is started and stopped and when a print queue is put on hold.
- A print queue log records information such as the name of users who submitted jobs and the size of each job.

You can view print service logs using Server Admin.

To view Print service logs:

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click Print.

4 Click Logs.

Use the Filter field to search for specific entries.

From the Command Line

You can also view the logs by using the `cat` or `tail` command in Terminal. For more information, see the Print service chapter of *Command-Line Administration*.

From the Command Line:

```
# View Print service logs
tail /Library/Logs/PrintService/PrintService_admin.log
```

Securing Multimedia Services

27

Use this chapter to learn how to secure Multimedia services.

Protecting QuickTime multimedia streams and only allowing access to those who are authorized to view them can help keep information private. The following section helps you understand and configure QuickTime Streaming Server (QTSS) securely.

Streaming is the delivery of media, such as movies and live presentations, over a network in real time. A computer (streaming server) sends the media to another computer (client computer), which plays the media as it is delivered.

With QTSS software, you can deliver:

- Broadcasts of live events in real time
- Video on demand
- Playlists of prerecorded content

A level of security is inherent in real-time streaming, because content is delivered only as the client needs it and no files remain afterward, but you might need to address some security issues.

For more information about configuring multimedia services, see the *QuickTime Streaming Server and Broadcasting Administration* guide.

Disabling QTSS

If your server is not intended to be a QuickTime streaming server, disable the QuickTime Streaming server software. Disabling the software prevents potential vulnerabilities on your computer. QTSS is disabled by default, but verification is recommended.

To disable QTSS:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.

3 In the expanded Servers list, click QuickTime Streaming.

4 Click Stop QuickTime Streaming (below the Servers list).

From the Command Line:

```
# ------------------------------------------------------------------
# Securing Multimedia Services
# ------------------------------------------------------------------

# Disable QTSS
serveradmin stop qtss
```

Securely Configuring QTSS

A level of security is inherent in real-time streaming because content is delivered only as the client needs it and no files remain afterward. However, you might need to address some security issues.

The streaming server uses the IETF standard RTSP/RTP protocols. RTSP runs on top of TCP and RTP runs on UDP. Many firewalls are configured to restrict TCP packets by port number, and are very restrictive on UDP.

There are three options for streaming through firewalls with QTSS. These options are not mutually exclusive. Typically one or more are used to provide the most flexible setup. The three configurations outlined below are for clients behind a firewall.

- **Stream via port 80.** This option enables the streaming server to encapsulate RTSP and RTP traffic inside TCP port 80 packets. Because this is the default port used for HTTP-based web traffic, the streamed content gets through most firewalls. However, encapsulating the streaming traffic lowers performance on the network and requires faster client connections to maintain streams. It also increases load on the server.
- **Open the appropriate ports on the firewall.** This option allows the streaming server to be accessed via RTSP/RTP on the default ports, and provides better use of network resources, lower speeds for client connections, and less load on the server. The ports that must be open include:
 - TCP port 80: Used for signaling and streaming RTSP/HTTP (if enabled on server).
 - TCP port 554: Used for RTSP.
 - UDP ports 6970–9999: Used for UDP streaming. A smaller range of UDP ports, typically 6970-6999, can usually be used.
 - TCP port 7070: Optionally used for RTSP. (Real Server uses this port; QTSS/Darwin can also be configured to use this port.)
 - TCP ports 8000 and 8001: Can be opened for Icecast MP3 streaming.

- **Set up a streaming proxy server.** The proxy server is placed in the network demilitarized zone (DMZ)—an area on the network that is between an external firewall that connects to the Internet and an internal firewall between the DMZ and the internal network.

 Using firewall rules, packets with the ports defined above are allowed from the proxy server to clients through the internal firewall, and also between the proxy server and the Internet via the external firewall. However, clients are not allowed to make direct connections to external resources over those ports.

 This approach ensures that all packets bound for the internal network come through the proxy server, providing an additional layer of network security.

Configuring a Streaming Server

If you require QTSS, configure it in conjunction with your firewall and bind it to a single IP address.

To configure a streaming server:

1. Open Server Admin.
2. In the Computers & Services list, click QuickTime Streaming for the server.
3. Click Settings.
4. Click IP Binding.

 By binding QTSS with an IP address, you can easily track network activity. You can also configure the firewall to restrict network access to this IP address. IP binding is also helpful when your server is multihomed (for example, if you're also hosting a web server).
5. Select the IP address from the list.
6. Click Save.
7. Start Service.

From the Command Line:

```
# Configure a streaming server
serveradmin settings
     qtss:server:bind_ip_addr:_array_index:0 = "$Bind_IP_Address"
```

Serving Streams Through Firewalls Using Port 80

If you are setting up a streaming server on the Internet and some of your clients are behind firewalls that allow only web traffic, enable streaming on port 80.

With this option, the streaming server accepts connections on port 80, the default port for web traffic, and QuickTime clients can connect to your streaming server even if they are behind a web-only firewall.

If you enable streaming on port 80, make sure you disable any web server with the same IP address to avoid conflicts with your streaming server.

To serve QuickTime streams over HTTP port 80:

1. In Server Admin, click QuickTime Streaming under the server in the Servers list.
2. Click Settings.
3. Click IP Bindings.
4. Select "Enable streaming on port 80."

Important: If you enable streaming on port 80, make sure your server is not also running a web server, such as Apache. Running QTSS and a web server with streaming on port 80 enabled can cause a port conflict that results in one or both servers not behaving properly.

From the Command Line:

```
# Serve QuickTime streams over HTTP port 80
$ serveradmin settings
     qtss:server:rtsp_port:_array_index:0 = 554
     qtss:server:rtsp_port:_array_index:1 = 80
     qtss:server:rtsp_port:_array_index:2 = 8000
     qtss:server:rtsp_port:_array_index:3 = 8001
```

Streaming Through Firewalls or Networks with Address Translation

The streaming server sends data using UDP packets. Firewalls designed to protect information on a network often block UDP packets. As a result, client computers located behind a firewall that blocks UDP packets can't receive streamed media.

However, the streaming server also allows streaming over HTTP connections, which allows streamed media to be viewed through even very tightly configured firewalls.

Some client computers on networks that use address translation cannot receive UDP packets, but they can receive media that's streamed over HTTP connections.

If users have problems viewing media through a firewall or via a network that uses address translation, have them upgrade their client software to QuickTime 5 or later. If users still have problems, have their network administrators provide them with the relevant settings for the streaming proxy and streaming transport settings on their computers.

Network administrators can also set firewall software to permit RTP and RTSP throughput.

Changing the Password Required to Send an MP3 Broadcast Stream

Broadcasting MP3s to another server requires authentication.

To change the MP3 broadcast password:

1. In Server Admin, click QuickTime Streaming under the server in the Servers list.
2. Click Settings, then click Access.
3. In the MP3 Broadcast Password box, enter a new password.
4. Click Save.

From the Command Line:

```
# Change the MP3 broadcast password
serveradmin settings
qtss:modules:_array_id:QTSSMP3StreamingModule:mp3_broadcast_password =
     "password"
```

Using Automatic Unicast (Announce) with QTSS on a Separate Computer

You can broadcast from QuickTime Broadcaster to QTSS. This setting can also be used to receive Announced UDP streams from another QuickTime streaming server via a relay using the Automatic Unicast (Announce) transmission method. To do so, you must create a broadcast user name and password on the streaming server.

To create a broadcast user name and password on the streaming server:

1. In Server Admin, click QuickTime Streaming under the server in the Servers list.
2. Click Settings, then click Access.
3. Click the "Accept incoming broadcasts" checkbox.
4. Click Set Password and enter the name and password.
5. Click Save.

From the Command Line:

```
# Create a broadcast user name and password on the streaming server
serveradmin settings
     qtss:modules:_array_id:QTSSReflectorModule:allow_broadcasts = yes
```

Controlling Access to Streamed Media

You can set up authentication to control client access to streamed media files. You can use Workgroup Manager to specify who can access the media files, or you can use an access file.

To control access using Open Directory:

- Authorize each user in Workgroup Manager.

 For more information, see *Open Directory Administration*.

To control access using an access file:

Two schemes of authentication are supported: basic and digest. By default, the server uses the more secure digest authentication.

You can also control playlist access and administrator access to your streaming server. Authentication does not control access to media streamed from a relay server. The administrator of the relay server must set up authentication for relayed media.

The ability to manage user access is built into QTSS, so it is always enabled.

For access control to work, an access file must be present in the directory you selected as your media directory. If an access file is not present in the QTSS media directory, all clients are allowed access to the media in the directory.

1. Use the qtpasswd command-line utility to create user accounts with passwords.
2. Create an access file and place it in the media directory you want to protect.
3. To disable authentication for a media directory, remove the access file (named qtaccess) or rename it (for example, qtaccess.disabled).

Creating an Access File

An access file is a text file named qtaccess that contains information about users and groups who are authorized to view media in the directory where the access file is stored.

The directory you use to store streamed media can contain other directories, and each directory can have its own access file.

When a user tries to view a media file, the server checks for an access file to see whether the user is authorized to view the media. The server looks first in the directory where the media file is located. If an access file is not found, it looks in the enclosing directory.

The first access file that's found is used to determine whether the user is authorized to view the media file.

The access file for the streaming server works like the Apache web server access file.

You can create an access file with a text editor. The filename must be qtaccess and the file can contain some or all of the following information:

```
AuthName <message>
AuthUserFile <user filename>
AuthGroupFile <group filename>
```

```
require user <username1> <username2>
require group <groupname1> <groupname2>
require valid-user
require any-user
```

Terms not in angle brackets are keywords. Anything in angle brackets is information you supply.

Save the access file as plain text (not .rtf or any other file format).

Here's a brief explanation of each keyword:

- `message` is text your users see when the login window appears. It's optional. If your message contains white space (such as a space character between terms), enclose the message in quotation marks.
- `user filename` is the path and filename of the user file. For Leopard, the default is /Library/QuickTimeStreaming/Config/qtusers.
- `group filename` is the path and filename of the group file. For Leopard, the default is /Library/QuickTimeStreaming/Config/qtgroups. A group file is optional. If you have many users, it might be easier to set up groups and then enter the group names, instead of listing each user.
- `username` is a user who is authorized to log in and view the media file. The user's name must be in the user file you specified. You can also specify `valid-user`, which designates any valid user.
- `groupname` is a group whose members are authorized to log in and view the media file. The group and its members must be listed in the group file you specified.

You can use these additional user tags:

- `valid-user` is any user defined in the qtusers file. The statement "require valid-user" specifies that any authenticated user in the qtusers file can have access to the media files. If this tag is used, the server prompts users for user name and password.
- `any-user` allows any user to view media without providing a name or password.
- `AuthScheme` is a keyword with the values "basic" or "digest" to a qtaccess file. This overrides the global authentication setting on a directory-by-directory basis.

If you make customized changes to the default qtaccess access file, be aware that making changes to broadcast user settings in Server Admin will modify the default qtaccess file at the root level of the movies directory. Therefore, customized modifications you make are not preserved.

What Clients Need When Accessing Protected Media

Users must have QuickTime 5 or later to access a media file that digest authentication is enabled for. If your streaming server is set up to use basic authentication, users need QuickTime 4.1 or later. Users must enter their user names and passwords to view the media file. Users who try to access a media file with an earlier version of QuickTime will see the error message "401: Unauthorized."

Adding User Accounts and Passwords

You can add a user account and password if you log in to the server computer.

To add a user account:

1. Log in to the server computer as root, open a terminal window, and enter the following:

 `qtpasswd <user-name>`

 Alternatively, use `sudo` to execute the command as root.
2. Enter a password for the user and reenter it when prompted.

From the Command Line:

```
# Add a user account
qtpasswd $USER
```

Adding or Deleting Groups

You can edit the /Library/QuickTimeStreaming/Config/qtgroups file with any text editor as long the file uses this format:

`<groupname>: <user-name1> <user-name2> <user-name3>`

For Windows, the path is c:\Program Files\Darwin Streaming Server\qtgroups. For other supported platforms, it is /etc/streaming/qtgroups.

To add or delete a group, edit the group file you set up.

From the Command Line:

```
# Adding groups
echo "$GROUP_NAME: $USER1 $USER2 $USER3" /Library/QuickTimeStreaming/
     Config/qtgroups
```

Making Changes to the User or Group File

You can make changes to the user or group file if you log in to the server computer.

To delete a user from a user or group file:

1. Log in to the server computer as administrator and use a text editor to open the user or group file.
2. Delete the user name and encrypted passwords line from the user file.
3. Delete the user name from the group file.

To change a user password:

1. Log in to the server computer as root, open a terminal window, and enter the following:

   ```
   qtpasswd <user-name>
   ```

 Alternatively, use `sudo` to execute the command as root.
2. Enter a new password for the user.

 The password you enter replaces the password in the file.

From the Command Line:

```
# Change a user password
qtpasswd $USER
```

Viewing QTSS Logs

QTSS provides the following log files:

- **Error logs.** These log files record errors such as configuration problems. For example, if you bind to a specific IP address that can't be found, or a if user deletes streaming files, these items are logged.
- **Access logs.** When someone plays a movie streamed from your server, the log reports such information as the date, time, and IP address of the computer that played the movie.

QTSS log files are stored in /Library/QuickTimeStreaming/Logs.

QTSS keeps its logs in standard W3C format, allowing you to use a number of popular log analysis tools to parse the data.

To view the QTSS log:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. Click QuickTime Streaming.
4. Click Logs and then choose a log from the View pop-up menu.

From the Command Line:

```
# View the QTSS log
tail /Library/QuickTimeStreaming/Logs/$LOG_FILE
```

Securing Grid and Cluster Computing Services

28

Use this chapter to learn how to secure Grid and Cluster Computing services.

Protecting grid and cluster services helps control your network's free CPU cycles from misuse. This chapter helps you restrict your network's CPUs to authorized users.

Xgrid, a technology in Leopard Server and Leopard, simplifies deployment and management of computational grids. Xgrid enables you to group computers into grids or clusters, and allows users to easily submit complex computations to groups of computers (local, remote, or both), as an ad hoc grid or a centrally managed cluster.

For more information about configuring multimedia services, see the *Xgrid Administration* guide.

Understanding Xgrid Service

Xgrid service handles the transferring of computing jobs to the grid and returns the results. Xgrid does not calculate anything, does not know anything about calculating, does not have content for calculating, and does not even know that you are calculating anything.

The computing job is handled by software (such as perl) that runs on the network computers, can be installed before running the computing job, or is transferred to the computers using Xgrid.

The primary components of a computational grid perform the following functions:

- An agent runs one task at a time per CPU. (A dual-processor computer can run two tasks simultaneously.)
- A controller queues tasks, distributes those tasks to agents, and handles task reassignment.
- A client submits jobs to the Xgrid controller in the form of multiple tasks. (A client can be any computer running Tiger or later or Server Tiger or later.)

In principle, the agent, controller, and client can run on the same server, but it is often more efficient to have a dedicated controller node.

Disabling Xgrid Service

If your server is not intended to be an Xgrid server, disable the Xgrid server software. Disabling the software prevents potential vulnerabilities on your computer.

The Xgrid service is disabled by default, but verification is recommended.

To disable Xgrid service:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select Server.
4. Click Settings.
5. Click Services.
6. Deselect Xgrid.
7. Click Save.

From the Command Line:

```
# ------------------------------------------------------------------
# Xgrid Service
# ------------------------------------------------------------------

# Disable Xgrid service
serveradmin stop xgrid
```

Authentication Methods for Xgrid

You can configure Xgrid with or without authentication. If you require authentication of controllers to mutually authenticate with clients and agents, you can choose Single Sign-On or Password-Based Authentication.

You set up an Xgrid controller using Server Admin. You can specify the type of authentication for agents and clients. The passwords entered in Server Admin for the controller must match those entered for each agent and client.

When establishing passwords for agents and clients, consider these points:

- **Kerberos authentication (single sign-on).** If you use Kerberos authentication for agents or clients, the server that's the Xgrid controller must be configured for Kerberos, must be in the same realm as the server running the Kerberos domain controller (KDC) system, and must be bound to the Open Directory master.

 The agent uses the host principal found in the /etc/krb5.keytab file. The controller uses the Xgrid service principal found in the /etc/krb5.keytab file.
- **Agents.** The agent determines the authentication method. The controller must conform to that method and password (if a password is used). When an agent is configured with a standard password (not single sign-on), you must use the same password for agents when you configure the controller. If the agent has specified single sign-on, the correct service principal and host principals must be available.
- **Clients.** If your server is the controller for a grid, be sure that Leopard and Leopard Server clients use the correct authentication method for the controller.

 A client cannot submit a job to the controller unless the user chooses the correct authentication method and enters their password correctly, or has the correct ticket-granting ticket from Kerberos.

For more information, see *Xgrid Administration and High Performance Computing*.

Single Sign-On

Single sign-on (SSO) is the most powerful and flexible form of authentication. It leverages the Open Directory and Kerberos infrastructures in Leopard Server to manage authentication behind the scenes, without user intervention.

Each Xgrid participant must have a Kerberos principal. The clients and agents obtain ticket-granting tickets for their principal, which is used to obtain a service ticket for the controller service principal. The controller looks at the ticket granted to the client to determine the user's principal and verifies it with the relevant service access control lists (SACLs) and groups to determine privileges.

Generally, you should use this option if any of the following conditions are true:

- You already have single sign-on in your environment.
- You have administrator control over all agents and clients in use.
- Jobs must run with special privileges (such as for local, network, or SAN file system access).

Password-Based Authentication

When you can't use single sign-on, you can require password authentication. You may not be able to use single sign-on if:

- Potential Xgrid clients are not trusted by your single sign-on domain (or you don't have one)
- You want to use agents across the Internet or that are outside your control
- It is an ad hoc grid, without the ability to prearrange a web of trust

In these situations, your best option is to specify a password. You have two password options: one for controller-client and one for controller-agent. For security reasons, these should be different passwords.

Note: You can also create hybrid environments, such as with client-controller authentication done using passwords but controller-agent authentication done using single sign-on (or vice versa).

No Authentication

The No Authentication method creates potential security risks, because anyone can connect or run a job, which can expose sensitive data. This option is appropriate only for testing a private network in a home or lab that is inaccessible from any untrusted computer, or when none of the jobs or the computers contain sensitive or important information.

Securely Configuring Xgrid Service

Xgrid service must be running for your server to control a grid or participate in a grid as an agent. If Xgrid service is required, configure the Xgrid agent and controller. The Xgrid controller and agent are disabled by default.

When configuring the Xgrid agent and controller, require authentication to protect your network from malicious users. Authentication requires that agent and controller use the same password or authenticate using Kerberos single sign-on. With no authentication, a malicious agent could receive tasks and potentially access sensitive data.

Configuring an Xgrid Agent

An Xgrid agent runs the computational tasks of a job. In Leopard Server, the agent is turned off by default. When an agent is turned on and becomes active at startup, it registers with a controller. (An agent can be connected to only one controller at a time.) The controller sends instructions and data to the agent for the controller's jobs. After it receives instructions from the controller, the agent executes its assigned tasks and sends the results back to the controller.

You use Server Admin to set up your server as an Xgrid agent. In addition, you can associate the agent with a specific controller or permit it to join a grid, specify when the agent accepts tasks, and set a password that the controller must recognize.

To configure an Xgrid agent on the server:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click Xgrid.
4. Click Settings.
5. Click Agent.
6. Click "Enable agent service."
7. Specify a controller by choosing its name in the Controller pop-up menu or by entering the controller name.

 By default, the agent uses the first available controller.

 Note: An agent can find a controller in one of three ways: a specific hostname or IP address, the first available controller that advertises on Bonjour on the local subnet, or by a specific Bonjour service name.service lookup against the domain name server for _xgrid._tcp._ip.
8. Specify when the agent will accept tasks.

 Tasks can be accepted when the computer is idle or always.

 A computer is considered idle when it has no mouse or keyboard input and ignores CPU and network activity. If a user returns to a computer that is running a grid task, the computer continues to run the task until it is finished.
9. From the pop-up menu, choose one of the following authentication options and enter the password.
 - **Password** requires that the agent and controller use the same password.
 - **Kerberos** uses SSO authentication for the agent's administrator.
 - **None** does not require a password for the agent. This option is *not* recommended because it provides no protection from unapproved use of your grid. With no authentication, an unapproved agent could receive tasks and potentially access sensitive data.
10. Click Save.

 Important: If you require authentication, the agent and controller must use the same password or must authenticate using Kerberos single sign-on.

From the Command Line:

```
# Configure an Xgrid agent on the server
/usr/sbin/xgridctl agent stop
```

Configuring an Xgrid Controller

You use Server Admin to configure an Xgrid controller. When configuring the controller, you can also set a password for any agent using the grid and for any client that submits a job to the grid.

To configure an Xgrid controller:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. In the expanded Servers list, click Xgrid.
4. Click Settings.
5. Click Controller.
6. Click "Enable controller service."
7. From the Client Authentication pop-up menu, choose one of the following authentication options for clients and enter the password.
 - **Password** requires that the agent and controller use the same password.
 - **Kerberos** uses sign-on authentication for the agent's administrator.
 - **None** does not require a password for the agent. This option is *not* recommended because it provides no protection from unapproved use of your grid. With no authentication, an unapproved agent could receive tasks and potentially access sensitive data.
8. Click Save.

 Important: If you require authentication, the agent and controller must use the same password or must authenticate using Kerberos single sign-on.

From the Command Line:

```
# Configure an Xgrid controller
serveradmin settings xgrid:ControllerSettings:Enabled = yes
serveradmin settings xgrid:ControllerSettings:prefs:ClientAuthentication =
     Password
serveradmin settings xgrid:ControllerSettings:ClientPassword =
     $Xgrid_Client_Password
```

Managing Who Can Obtain Administrative Privileges (sudo)

29

Use this chapter to restrict administrator access to the sudo command by specifying who can use this command in the sudoers file.

The `sudo` command gives root user privileges to users specified in the sudoers file. If you're logged in as an administrator user and your username is specified in the /etc/sudoers file, you can use this command.

Managing the sudoers File

Limit the list of administrators allowed to use the `sudo` tool to those administrators who require the ability to run commands with root user privileges.

To change the /etc/sudoers file:

1. Edit the /etc/sudoers file using the `visudo` tool, which allows for safe editing of the file, then run the following command with root user privileges:

   ```
   $ sudo visudo
   ```

2. When prompted, enter your administrator password.

 There is a timeout value associated with the `sudo` tool. This value indicates the number of minutes until `sudo` prompts for a password again.

 The default value is 5, which means that after issuing the `sudo` command and entering the correct password, additional `sudo` commands can be entered for 5 minutes without reentering the password. This value is set in the /etc/sudoers file.

 For more information, see the `sudo` and `sudoers` man pages.

3. In the Defaults specification section of the file, add the following line:

   ```
   Defaults timestamp_timeout=0
   ```

4 Restrict which administrators are allowed to run the `sudo` tool by removing the line that begins with `%admin` and adding the following entry for each user, substituting the user's short name for the word *`user`*:

```
user ALL=(ALL) ALL
```

Doing this means that when an administrator is added to a system, the administrator must be added to the /etc/sudoers file as described above if that administrator needs to use the `sudo` tool.

5 Save and quit `visudo`.

For more information, see the `pico` and `visudo` man pages.

Managing Authorization Through Rights

30

Use this chapter to control authorization on your system by managing the policy database.

Authorization on Leopard and Leopard Server is controlled by a policy database. This database is stored in /etc/authorization. The database format is described in comments at the top of that file.

The SecurityAgent plug-in processes all requests for authentication by gathering requirements from the policy database (/etc/authorization).

Actions can be successfully performed only when the user has acquired the rights to do so.

Understanding the Policy Database

The policy database is a property list that consists of two dictionaries:

- The rights dictionary
- The rules dictionary

The Rights Dictionary

The rights dictionary contains a set of key/value pairs, called *right specifications*. The key is the *right name* and the value is information about the right, including a description of what the user must do to acquire the right.

The following is an extract from the policy database installed on your system.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC …>
<plist version="1.0">
<dict>
…
  <key>rights</key>
  <dict>
     <key></key>
     <dict>
```

```
        <key>class</key>
        <string>rule</string>
        <key>comment</key>
        <string>Matches otherwise unmatched rights (i.e., is a default).</
string>
        <key>rule</key>
        <string>default</string>
</dict>
<key>system.device.dvd.setregion.initial</key>
<dict>
        <key>class</key>
        <string>user</string>
        <key>comment</key>
        <string>Used by the DVD player to set the region code the first
time. Note that changing the region code after it has been set requires
a different right (system.device.dvd.setregion.change).</string>
        <key>group</key>
        <string>admin</string>
        <key>shared</key>
        <true/>
</dict>
…
<key>config.add.</key>
<dict>
        <key>class</key>
        <string>allow</string>
        <key>comment</key>
        <string>Wildcard right for adding rights. Anyone is allowed to add
any (non-wildcard) rights.</string>
</dict>
…
```

In this extract from the policy database, there are three rights:

- The right specification with an empty key string is known as the default right specification. To obtain this right a user must satisfy the default rule which, by default on current versions of Mac OS X, is to prove that they are an administrator.
- `system.device.dvd.setregion.initial` controls whether the user is allowed to set the initial region code for the DVD drive. By default, a user must prove that they are an administrator (in group admin) to set the DVD region.
- `config.add.` is a wildcard right specification (it ends with a dot) that matches any right whose name starts with the `config.add.` characters. This right controls whether a user can add a right specification to the policy database. By default, any user can add a right specification.

When a program asks for a right, Authorization Services executes the following algorithm:

1. It searches the policy database for a right specification whose key matches the right name.
2. If that fails, it searches the policy database for a wildcard right specification whose key matches the right name. If multiple rights are present, it uses the one with the longest key.
3. If that fails, it uses the default right specification.

After it has found the relevant right specification, Authorization Services evaluates the specification to decide whether to grant the right. In some cases this is easy (in the extract from the policy database above, `config.add.` is always granted), but in other cases it can be more complex (for example, setting the DVD region requires that you enter an administrator password).

Rules

A rule consists of a set of attributes. Rules are preconfigured when Leopard Server is installed, but applications can change them at any time.

The following table describes the attributes defined for rules.

Rule attribute	Generic rule value	Description
key		The key is the name of a rule. A key uses the same naming conventions as a right. Security Server uses a rule's key to match the rule with a right. Wildcard keys end with a '.'. The generic rule has an empty key value. Any rights that do not match a specific rule use the generic rule.
group	admin	The user must authenticate as a member of this group. This attribute can be set to any one group.
shared	true	If this is set to true, Security Server marks the credentials used to gain this right as shared. Security Server can use any shared credentials to authorize this right. For maximum security, set sharing to false so credentials stored by Security Server for one application are not used by another application.
timeout	300	The credential used by this rule expires in the specified number of seconds. For maximum security where the user must authenticate every time, set the timeout to 0. For minimum security, remove the timeout attribute so the user authenticates only once per session.

There are some specific rules in the policy database for Mac OS X applications. There is also a generic rule in the policy database that the Security Server uses for any right that doesn't have a specific rule.

Managing Authorization Rights

Managing authorization rights involves creating and modifying right and rule values.

Creating an Authorization Right

To authorize a user for specific rights, you must create an authorization right in the `rights` dictionary. Each right consists of the following:

- The name of the right
- A value that contains optional data pertaining to the right
- The byte length of the value field
- Optional flags

The right always matches up with the generic rule unless a new rule is added to the policy database.

Modifying an Authorization Right

To modify a right, change the relevant value in /etc/authorization and save the file:

- To lock out all privileged operations not explicitly allowed, change the generic rule by setting the timeout attribute to 0.
- To allow privileged operations after the user is authorized, remove the timeout attribute from the generic rule.
- To prevent applications from sharing rights, set the shared attribute to false.
- To require users to authenticate as a member of the staff group instead of the admin group, set the group attribute to staff.

Note: There are APIs that you can use for modifying /etc/authorization. It's better to use these APIs than to manually change the values.

Example Authorization Restrictions

As an example of how the Security Server matches a right with a rule in the policy database, consider a grades-and-transcripts application.

The application requests the right com.myOrganization.myProduct.transcripts.create. Security Server looks up the right in the policy database. Not finding a match, Security Server looks for a rule with a wildcard key set to com.myOrganization.myProduct.transcripts., com.myOrganization.myProduct., com.myOrganization., or com.—in that order—checking for the longest match.

If no wildcard key matches, Security Server uses the generic rule.

Security Server requests authentication from the user. The user provides a user name and password to authenticate as a member of the group admin. Security Server creates a credential based on the user authentication and the right requested.

The credential specifies that other applications can use it, and Security Server sets the expiration to five minutes.

Three minutes later, a child process of the application starts up. The child process requests the right com.myOrganization.myProduct.transcripts.create.

Security Server finds the credential, sees that it allows sharing, and uses the right. Two and a half minutes later, the same child process requests the right com.myOrganization.myProduct.transcripts.create again, but the right has expired.

Security Server begins the process of creating a new credential by consulting the policy database and requesting user authentication.

Maintaining System Integrity

31

Use this chapter to learn how to maintain system integrity.

Monitoring events and logs can help protect the integrity of your computer.

Using auditing and logging tools to monitor your computer can help you secure your computer. By reviewing these audits and log files, you can stop login attempts from unauthorized users or computers and further protect your configuration settings. This chapter also discusses antivirus tools, which detect unwanted viruses.

Using Digital Signatures to Validate Applications and Processes

A digital signature uses public key cryptography to ensure the integrity of data. Like traditional signatures written with ink on paper, they can be used to identify and authenticate the signer of the data.

However, digital signatures go beyond traditional signatures in that they can also ensure that the data itself has not been altered. This is like designing a check in such a way that if someone alters the amount of the sum written on the check, an "Invalid" watermark becomes visible on the face of the check.

To create a digital signature, the signer generates a message digest of the data and then uses a private key to sign the digest. The signer must have a valid digital certificate containing the public key that corresponds to the private key. The combination of a certificate and related private key is called an identity. The signature includes the signed digest and information about the signer's digital certificate. The certificate includes the public key and the algorithm needed to verify the signature.

To verify that the signed document has not been altered, the recipient uses the algorithm to create message digest and applies the public key to the signed digest. If the two digests prove identical, the message cannot have been altered and must have been sent by the owner of the public key.

To ensure that the person who provided the signature is not only the same person who provided the data but is also who they say they are, the certificate is also signed—in this case by the certificate authority (CA) who issued the certificate.

Signed code uses several digital signatures:

- If the code is universal, the object code for each architecture is signed separately.
- Components of the application bundle (such as the Info.plist file, if there is one) are also signed.

Validating Application Bundle Integrity

To validate the signature on a signed application bundle, use the `codesign` command with the `-v` option.

From the Command Line:

```
# ------------------------------------------------------------------
# Maintaining System Integrity
# ------------------------------------------------------------------

# Validate application bundle integrity.
codesign -v $code_path
```

This command checks that the code binaries at *`code-path`* are signed, that the signature is valid, that sealed components are unaltered, and that the bundle passes basic consistency checks. It does not verify that the code satisfies any requirements except its own designated requirement.

To verify a requirement, use the `-R` option. For example, to verify that the Apple Mail application is identified as Mail, signed by Apple, and secured with Apple's root signing certificate, use the following command:

From the Command Line:

```
# Verify a requirement.
codesign -v -R="identifier com.apple.Mail and anchor apple" /Applications/
     Mail.app
```

Unlike the `-r` option, the `-R` option takes only a single requirement rather than a requirements collection (no => tags). Add additional `-v` options to get details on the validation process.

For more information about signing and verifying application bundle signatures, see *Code Signing Guide* at developer.apple.com/documentation/Security/ Conceptual/ CodeSigningGuide. For more information about the `codesign` command, see its man page.

Validating Running Processes

You can also use `codesign` to validate the signatures of running processes.

If you pass a number rather than a path to the verify option, `codesign` takes the number to be the process ID (pid) of a running process, and performs dynamic validation instead.

Auditing System Activity

Auditing is the capture and maintenance of information about security-related events. Auditing helps determine the causes and methods used for successful and failed access attempts.

The audit subsystem allows authorized administrators to create, read, and delete audit information. The audit subsystem creates a log of auditable events and allows the administrator to read all audit information from the records in a manner suitable for interpretation. The default location for these files is the /var/audit/ folder.

The audit subsystem is controlled by the `audit` utility located in the /usr/sbin/ folder. This utility transitions the system in and out of audit operation.

The default configuration of the audit mechanism is controlled by a set of configuration files in the /etc/security/ folder.

If auditing is enabled, the /etc/rc startup script starts the audit daemon at system startup. All features of the daemon are controlled by the audit utility and audit_control file.

Installing Auditing Tools

The Common Criteria Tools disk image (.dmg) file contains the installer for auditing tools. This disk image file is available from the Common Criteria webpage located at www.apple.com/support/security/commoncriteria/.

After downloading the Common Criteria Tools disk image file, copy it to a removable disk, such as a CD-R disc, FireWire disk, or USB disk.

To install the Common Criteria Tools software:

1. Insert the disk that contains the Common Criteria Tools disk image file and open the file to mount the volume containing the tools Installer.
2. Double-click the CommonCriteriaTools.pkg installer file.
3. Click Continue, then proceed through the installation by following the onscreen instructions.
4. When prompted to authenticate, enter the user name and password of the administrator account.

From the Command Line:

```
# Install the common criteria tools software
installer -pkg CommonCriteriaTools.pkg -target /
```

Enabling Auditing

Modify the hostconfig file to enable auditing.

To turn auditing on:

1. Open Terminal.
2. Enter the following command to edit the /etc/hostconfig file.

   ```
   $ sudo pico /etc/hostconfig
   ```

3. Add the following entry to the file.

   ```
   AUDIT=-YES-
   ```

4. Save the file.

Auditing is enabled when the computer starts up.

The following table shows the possible audit settings and what they do.

Parameter	Description
`AUDIT=-YES-`	Enable auditing; ignore failure.
`AUDIT=-NO-`	Disable auditing.
`AUDIT=-FAILSTOP-`	Enable auditing; processes may stop if failure occurs.
`AUDIT=-FAILHALT-`	Enable auditing; the system halts if failure occurs.

If the `AUDIT` entry is missing from the /etc/hostconfig file, auditing is turned off. A failure is any occurrence that prevents audit events from being logged.

The audit subsystem generates warnings when relevant events such as storage space exhaustion and errors in operation are recognized during audit startup or log rotation. These warnings are communicated to the audit_warn script, which can then communicate these events to the authorized administrator.

From the Command Line:

```
# Enable auditing
cp /etc/hostconfig /tmp/test

if /usr/bin/grep AUDIT /etc/hostconfig
then
  /usr/bin/sed "/^AUDIT.*/s//AUDIT=-YES-/g" /tmp/test > /etc/hostconfig
else
  /bin/echo AUDIT=-YES- >> /etc/hostconfig
fi
```

Setting Audit Mechanisms

The system startup scripts attempt to configure auditing early in the system startup process. After auditing is enabled, the settings for the audit mechanism are set with the /etc/security/audit_control configuration file.

Files containing audit settings can be edited with any text editor. Terminal can be used with `pico` or `emacs` text editor tools. For more information about using text editors with Terminal, see the `pico` or `emacs` man page.

Audit flags are defined in terms of audit classes. Audit flags can be for the whole system, or specific flags can be used for a particular user. Audit flags can include or exclude classes of events from the audit record stream based on the outcome of the event. For example, the outcome could be success, failure, or both.

When a user logs in, the system-wide audit flags from the audit_control file are combined with the user-specific audit flags (if any) from the audit_user file, and together establish the preselection mask for the user.

The preselection mask determines which events will generate audit records for a user. If the preselection mask is changed, restart the computer to ensure that all components are producing audit events consistently.

Using Auditing Tools

This section describes how to use auditing tools.

Using the audit Tool

Auditing is managed by the `audit` tool. The `audit` tool uses this syntax:

```
$ audit [-nst] [file]
```

The `audit` tool controls the state of the auditing subsystem. The optional file operand specifies the location of the audit_control input file. The default file is /etc/security/audit_control.

You can use the following options with the `audit` tool.

Parameter	Description
`-n`	Forces the audit system to close the existing audit log file and rotate to a new log file in a location specified in the audit control file.
`-s`	Specifies that the audit system should restart and reread its configuration from the audit control file. A new log file is created.
`-t`	Specifies that the audit system should terminate. Log files are closed and renamed to indicate the time of the shutdown.

For more information, see the `audit` man page.

Using the auditreduce Tool

The `auditreduce` tool enables you to select events that have been logged in audit records. Matching audit records are printed to the standard output in their raw binary form. If no filename is specified, the standard input is used by default.

The `auditreduce` tool follows this syntax:

```
$ auditreduce [-A] [-a YYYYMMDD[HH[MM[SS]]]] [-b YYYYMMDD[HH[MM[SS]]]]
     [-c flags] [-d YYYYMMDD] [-e euid] [-f egid] [-g rgid] [-r ruid]
     [-u auid] [-j id] [-m event] [-o object=value] [file …]
```

For more information, see the `auditreduce` man pages.

Parameter	Description
`-A`	Selects all records.
`-a`	`YYYYMMDD [HH[MM[SS]]]` Selects records that occurred on or after the specified date and time.
`-b`	`YYYYMMDD [HH[MM[SS]]]` Selects records that occurred before the specified date and time.
`-c`	`flags` Selects records matching the given audit classes, specified as a comma-separated list of audit flags.
`-d`	`YYYYMMDD` Selects records that occurred on a specified date. Cannot be used with `-a` or `-b` option flags.
`-e`	`euid` Selects records with the specified effective user.
`-f`	`egid` Selects records with the specified effective group.
`-g`	`gid` Selects records with the specified real group.
`-r`	`ruid` Selects records with the specified real user.

Parameter	Description
`-u`	`auid` Selects records with the specified audit ID.
`-j`	`id` Selects records having a subject token with matching ID.
`-m`	`event` Selects records with the specified event name or number.
`-o`	`object` = value `file` = Selects records containing the specified path name. `file` ="/usr" matches paths starting with usr. `file` ="~/usr" matches paths not starting with usr. `msgqid` = Selects records containing the specified message queue ID. `pid` = Selects records containing the specified process ID. `semid` = Selects records containing the specified semaphore ID. `shmid` = Selects records containing the specified shared memory ID.

To select all records associated with effective user ID root from the audit log /var/audit/20031016184719.20031017122634:

```
$ auditreduce -e root /var/audit/20031016184719.20031017122634
```

To select all setlogin events from that log:

```
$ auditreduce -m AUE_SETLOGIN /var/audit/20031016184719.20031017122634:
```

Using the praudit Tool

The `praudit` tool prints the contents of audit records. Audit records appear in standard output (stdout). If no filename is specified, standard input (stdin) is used.

The `praudit` tool uses this syntax:

```
$ praudit [options] audit-trail-file […]
```

You can use `praudit` with the following options:

Parameter	Description
`-l`	Prints the record in the same line. If this option is not specified, every token appears in a different line.
`-r`	Prints records in their raw format. This option is separate from `-s`.
`-s`	Prints the tokens in their short form. Short ASCII representations for record and event type are displayed. This option is separate from `-r`.
`del`	Specifies the delimiter. The default delimiter is the comma.

If raw or short form are not specified, tokens are printed in their long form. Events are displayed according to their descriptions given in audit_event, UIDs and GIDs are expanded to their actual ASCII representation, date and time is displayed in standard date format, and so on.

For more information, see the `praudit` man page.

Deleting Audit Records

You can clear the audit trail by deleting audit files using the command line.

> *WARNING:* You should not delete the currently active audit log.

To delete an audit file:

```
$ sudo srm /var/audit/20031016184719.20031017122634
```

Audit Control Files

The audit system uses the following text files to control auditing and write audit records. The default location for these files is the /etc/security/ folder.

- audit_class—The audit_class file contains descriptions of auditable event classes on the system. Each auditable event is a member of an event class. Each line maps an audit event mask (bitmap) to a class and a description.
- audit_control—The audit_control file contains several audit system parameters. Each line of this file is of the form `parameter:value`. Audit flags are a comma-delimited list of audit classes as defined in the audit_class file. Event classes can be preceded by a prefix that changes their interpretation.
- audit_event—The audit_event file contains descriptions of auditable events on the system. Each line maps an audit event number to a name, a description, and a class. Each event class should have a corresponding entry in the audit_class file.
- audit_user—The audit_user file specifies which audit event classes are to be audited for specific users. If specified, these flags are combined with system-wide audit flags in the audit_control file to determine which classes of events to audit for a user. These settings take effect when the user logs in. Each line maps a user name to a list of classes that should be audited and a list of classes that should not be audited.
- audit_warn—The audit_warn file runs when `auditd` generates warning messages. The default audit_warn is a script whose first parameter is the type of warning. The script appends its arguments to /etc/security/audit_messages. Administrators can replace this script with a more comprehensive one that takes different actions based on the type of warning. For example, a low-space warning could result in a mail message being sent to the administrator.

For more information about editing audit control files, see the *Common Criteria Administration* guide at www.apple.com/support/security.

Managing and Analyzing Audit Log Files

If auditing is enabled, the auditing subsystem adds records of auditable events to an audit log file. The name of an audit log file consists of the date and time it was created, followed by a period, and the date and time it was terminated. For example:

20040322183133.20040322184443.

This log was created on March 22, 2004 at 18:31:33 and was terminated on March 22, 2004 at 18:44:43.

The audit subsystem appends records to only one audit log file at a time. The currently active file has a suffix ".not_terminated" instead of a date and time. Audit log files are stored in the folders specified in the audit_control file. The audit subsystem creates an audit log file in the first folder specified.

When less than the minfree amount of disk space is available on the volume containing the audit log file, the audit subsystem:

1. Issues an audit_warn soft warning
2. Terminates the current audit log file
3. Creates a new audit log file in the next specified folder

After all folders specified have exceeded this minfree limit, auditing resumes in the first folder again. However, if that folder is full, an auditing subsystem failure can occur.

You can also choose to terminate the current audit log file and create a new one manually using the audit utility. This action is commonly referred to as "rotating the audit logs."

Use `audit -n` to rotate the current log file. Use `audit -s` to force the audit subsystem to reload its settings from the audit_control file (which also rotates the current log file).

Using Activity Analysis Tools

Leopard includes several command-line tools that you can use to analyze computer activity.

Depending on the tools' configurations and your computer's activity, running these tools can use large amounts of disk space. Additionally, these tools are only effective when other users don't have administrator access. Users with administrator access can edit logs generated by the tool and thereby circumvent the tool.

If your computer contains sensitive data, consider using both auditing and logging tools. By using both types of tools, you can research and analyze intrusion attempts and changes in your computer's behavior. You must configure these tools to meet your organization's needs, and then change their logging settings to create relevant information for reviewing or archiving purposes.

Validating System Logging

Logging is the recording of various events, including changes to service status, processes, and operating system components. Some events are security related, while others are information messages about your computer's activity. If an unexpected error occurs, you can analyze logs to help determine the cause of the error. For example, the logs might explain why a software update can't be installed, or why you can't authenticate.

Logging tools can be useful if you have multiple users who can access the `sudo` command. You can view logs to see what users did using the `sudo` command. Some `sudo` commands perform additional actions that are not logged. You should restrict the `sudo` commands that individual users are allowed to use. For more information, see "Managing the sudoers File" on page 369.

Use Console to view and maintain log files. Console is located in the /Applications/Utilities/ folder. Upon starting, the Console window shows the `console.log` file. Click Logs to display a pane that shows other log files on the system in a tree view. The tree view includes folders for services, such as web and mail server software.

In Leopard Server, log files are handled by the BSD subsystem or by a specific application. The BSD subsystem handles most important system logging, while some applications handle their own logging. Like other BSD systems, Leopard Server uses a background process called `syslogd` to handle logging.

A primary decision to make when configuring `syslogd` is whether to use local or remote logging. In local logging, log messages are stored on the hard disk. In remote logging, log messages are transferred over the network to a dedicated log server that stores them. Using remote logging is strongly recommended.

Configuring syslogd

The configuration file for the system logging process, `syslogd`, is /etc/syslog.conf. A manual for configuration of this file is available by issuing the command `man syslog.conf` in a Terminal window.

Each line in /etc/syslog.conf consists of text containing three types of data: a facility, a priority, and an action.

- Facilities are categories of log messages. Standard facilities include mail, news, user, and kern (kernel). Priorities deal with the urgency of the message. In order from least to most critical, they are: debug, info, notice, warning, err, crit, alert, and emerg.
- The priority of the log message is set by the application sending it, not by `syslogd`.
- The action specifies what to do with a log message of a specific facility and priority. Messages can be sent to files, named pipes, devices, or a remote host.

The following example specifies that for any log messages in the category "mail" with a priority of "emerg" or higher, the message is written to the /var/log/mail.log file:

```
mail.emerg /var/log/mail.log
```

The facility and priority are separated by a period, and these are separated from the action by tabs. Wildcards ("*") can also be used in the configuration file.

The following example logs all messages of any facility or priority to the file /var/log/all.log:

```
*.* /var/log/all.log
```

Local System Logging

The default configuration in /etc/newsyslog.conf is configured for local logging in the /var/log folder. The computer is set to rotate log files using the periodic `launchd` job according to time intervals specified in the /etc/newsyslog.conf file.

Rotation entails compressing the current log file, incrementing the integer in the filename of compressed log files, and creating a log file for new messages.

The following table describes the rotation process after two rotations.

Files before rotation	Files after first rotation	File after second rotation
system.log	system.log	system.log
mail.log	mail.log	mail.log
	mail.log.1.gz	mail.log.1.gz
	system.log.1.gz	system.log.1.gz
		mail.log.2.gz
		system.log.2.gz

Log files are rotated by a launchd job, and the rotation occurs if the computer is on when the job is scheduled. By default, log rotation tasks are scheduled between midnight and 1 in the morning, to be as unobtrusive as possible to users. If the system will not be powered on at this time, adjust the settings in /etc/newsyslog.conf.

For information about editing the /etc/newsyslog.conf file, issue the `man 5 newsyslog.conf` command in a Terminal window.

Remote System Logging

Using remote logging in addition to local logging is strongly recommended, because local logs can easily be altered if the system is compromised. Consider the following security issues when making the decision to use remote logging.

- The syslog process sends log messages in the clear, which could expose sensitive information.

- Too many log messages fill storage space on the logging system, rendering further logging impossible.
- Log files can indicate suspicious activity only if a baseline of normal activity is established, and if the files are regularly monitored for such activity.

If these security issues outweigh the security benefit of remote logging for the network being configured, do not use remote logging.

The following instructions assume a remote log server has been configured on the network.

To enable remote logging:

1. Open /etc/syslog.conf as root.
2. Add the following line to the top of the file, replacing `your.log.server` with the name or IP address of the log server, and making sure to keep all other lines intact:

   ```
   *.* @your.log.server
   ```

3. Exit, saving changes.
4. Send a hangup signal to `syslogd` to make it reload the configuration file:

   ```
   $ sudo killall -HUP syslogd
   ```

Viewing Logs in Server Admin

Server Admin provides logging for some services enabled on your server. A filter feature allows you to search through the log for specific information.

To view logs in Server Admin:

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

 The list of services appears.
3. From the expanded Servers list, select a service.
4. Click Logs.

 Some services have multiple logs associated with them.

From the Command Line:

```
# View logs in Server Admin
# Use tail or more to view the log files.
# The audit files are individually named based on the date.

/usr/bin/tail $AUDIT_FILE
```

Configuring the IPFW2 Firewall

32

Use this chapter to learn how configure the IPFW2 firewall.

Using a firewall to filter network traffic from a host or a network of hosts that are attempting to access your computer, prevents attackers from gaining access to your computer.

Firewall Protection

A Firewall is software that protects your Mac OS X computer from unauthorized users. When you turn firewall protection on, it is similar to erecting a wall to limit access to your computer. The firewall scans incoming network traffic and rejects or accepts these packets based on rules. You can restrict access to any network service running on your computer.

You can monitor activity involving your firewall by enabling firewall logging. Firewall logging creates a log file that tracks activity such as the sources and connection attempts blocked by the firewall. You can view this log in the Console utility.

The IPFW2 Firewall

Leopard includes the open source IPFW2 software as an alternate firewall. You use the `ipfw` command-line tool to filter packets by using rules to decide which packets to allow and which to deny.

The firewall scans incoming IP packets and rejects or accepts them based on the set of filters or rules you create. You can restrict access to any IP service running on your computer, and you can customize filters for all incoming addresses or for a range of IP addresses.

IPFW handles packets at a lower level of the networking stack than the Application firewall. Therefore, its rules take precedence over the Application firewall.

Configuring the IPFW Firewall

The IPFW2 firewall (also referred to here as IPFW) allows for the creation of complex and powerful packet filtering rulesets. This firewall can be difficult to configure, and can also disrupt network communications if improperly configured. It requires manually written rules, and the system must be configured to read those rules at startup. Configuring IPFW rulesets requires a higher level of expertise than many system administration tasks. If an administrator is not mindful of the IPFW ruleset on the system, confusion can arise when some network connectivity is not available that apparently should be.

Understanding IPFW Rulesets

An IPFW configuration or ruleset is a list of rules that are designed to match packets and take appropriate action. IPFW rules are numbered from 1 to 65535. The packet passed to the firewall is compared against each of the rules (in numerical order). When the packet matches a rule, the corresponding action is taken. A more complete description of the capabilities and configuration of IPFW can be found in the `ipfw` man page.

To view the currently enforced IPFW rules, run the command:

```
$ sudo ipfw print
```

The default output should appear something like this:

```
65535 allow ip from any to any
```

This line shows that the default configuration allows all traffic through the IPFW firewall, performing no filtering. Like all IPFW rules, it consists of a rule number (65535); an action (allow); and body (ip from any to any). In this case, the body (ip from any to any) matches all IP packets. This also happens to be a special rule, called the default rule. It is the highest-numbered rule possible and is compiled directly into the kernel. Because no rules have actually been added to the system, all packets are passed to this default rule, which allows them all through. However, if the Stealth Mode feature is enabled on the system, then the following line will appear first in the list:

```
33300 deny icmp from any to me in icmptypes 8
```

This rule shows the implementation of the Stealth Mode feature: dropping any incoming ping echo requests, which is ICMP type 8. Because it is a lower rule number (and thus also appears earlier when listed), it is consulted before the default rule.

With the exception of the Stealth Mode blocking of ping requests, the default configuration for IPFW on Mac OS X does not block any packets. Mac OS X relies primarily on the Application firewall to block unwanted network traffic. IPFW can be used to write complex and powerful rulesets, which make decisions about connectivity based on the form of the packet. The Application Firewall, on the other hand, makes decisions about connectivity based on whether the program trying to use the network is trusted. These two firewall technologies complement each other.

The next section describes how to make use of IPFW.

Implementing an IPFW Ruleset

Implementing an IPFW ruleset can be a challenging activity, filled with corner cases and problems that are difficult to debug. Because of this, administrators should develop a thorough understanding of a simple, strict ruleset and then carefully modify it to suit the needs of their particular network environment. This section first describes how to enable logging so that debugging is possible. Next, a simple ruleset is provided, and then ways in which it can be expanded are presented.

Enabling Firewall Logging

Even before implementing an IPFW ruleset, firewall logging should be enabled. This can be performed in the Security pane of System Preferences, and is described in the Firewall Settings section of "Securing Security Preferences." This setting enables logging for both the Application firewall and IPFW.

The system's ability to log packets can then be verified with the following command:

```
$ sudo sysctl net.inet.ip.fw.verbose
```

If the command returns a 2, then logging is enabled for both the Application firewall and IPFW. The system should now send both Application firewall and IPFW log messages to /var/log/appfirewall.log. These can be viewed using the Console program in /Applications/Utilities. Implementation of a basic ruleset can proceed, using the log to debug any connectivity failures that occur.

Implementing a Basic Inclusive Ruleset

An IPFW ruleset can be stored simply as a list of IPFW rules inside a text file. Traditionally, the file /etc/ipfw.conf is used to store these rules. Proper firewall ruleset design is inclusive: it allows only packets that match specific rules, and then denies all others. The following basic ruleset is inclusive and also very strict: it allows packets from other systems only when the host has initiated a connection to another system. This is appropriate for a client system that offers no network services to any other systems.

To implement this ruleset, enter the following rule in /etc/ipfw.conf file:

```
#Allow all traffic to us from our loopback interface
add 1000 allow all from any to any via lo0
```

```
#Allow all TCP packets out, and keep state in order to allow responses
add 10000 allow tcp from any to any out keep-state
#Allow all UDP packets out, and keep state in order to allow responses
add 12000 allow udp from any to any out keep-state
#Allow all ICMP traffic
add 20000 allow log icmp from any to any
#Allow DHCP packets in (use only if using DHCP)
add 60000 allow udp from any to any src-port 67 dst-port 68 in
#Reject all IP packets: anything not matched already will be dropped and
     logged
add 65534 deny log ip from any to any
#Allow all IP packets: here as a comment as a reminder of the default rule
#65535 allow ip from any to any
```

Once this ruleset is in /etc/ipfw.conf, it can be loaded with the command:

```
$ sudo /sbin/ipfw /etc/ipfw.conf
```

The following command can be issued to verify that the rules are loaded as expected:

```
$ sudo /sbin/ipfw print
```

Testing can now commence to determine whether the ruleset is compatible with your connectivity needs. If modifications are made to the ruleset in the file, the old rules must be flushed before your new rules are inserted. To flush the old rules and then re-insert a ruleset from /etc/ipfw.conf:

```
$ sudo /sbin/ipfw flush
$ sudo /sbin/ipfw /etc/ipfw.conf
```

Be sure to read the later section which describes the steps necessary to ensure that the rules in /etc/ipfw.conf are loaded at startup. Even if DHCP is not used, any unconnected interfaces may create log messages when they attempt to obtain IP settings from the computer. To eliminate these messages, configure those interfaces to "Off" using the Network preference pane.

Opening the Basic Ruleset to Permit Services

The basic ruleset described earlier does not permit the system to host any network services, such as Bonjour or Remote Login (SSH). This section describes rules that can be added to the firewall to allow the system to host some network services. Each of these rules should only be added if the system truly needs to offer the network service discussed. All possible network services cannot be covered here, but rules to allow other services should be available from other resources.

Add the following rules to allow Bonjour, substituting your local network and netmask for a.b.c.d/nm:

```
add 12600 allow udp from a.b.c.d/nm to any dst-port 5353
add 12601 allow udp from a.b.c.d/nm 5353 to any dst-port 1024-65535 in
```

Add the following rules to allow the Remote Login (SSH) service to be reached, substituting a.b.c.d/nm for networks you wish to allow:

```
add 12500 allow tcp from a.b.c.d/nm to any 22
add 12501 allow udp from a.b.c.d/nm to any 22
```

Add the following rules to allow the system to host File Sharing over AFP, substituting a.b.c.d/nm for networks you wish to allow:

```
add 12700 allow tcp from a.b.c.d/nm to any dst-port 548
```

Add the following rules to allow the Web Sharing service, substituting a.b.c.d/nm for networks you wish to allow:

```
add 14000 allow tcp from a.b.c.d/nm to any dst-port 80
add 14000 allow tcp from a.b.c.d/nm to any dst-port 443
```

Add the following rules to allow File Sharing over SMB, substituting your local network and netmask for a.b.c.d/nm:

```
add 12801 allow udp from a.b.c.d/nm 137,138,139 to me in keep-state
add 12803 allow tcp from a.b.c.d/nm 137,138,139 to me keep-state setup
```

Making the Basic Ruleset More Restrictive

The basic ruleset described earlier can be made more restrictive by making it specifically drop some types of packets.

To deny traffic addressed for the loopback interface but not originating from it (must be numbered after rule 1000 above):

```
add 1010 deny all from any to 127.0.0.0/8
```

To restrict ICMP traffic, you must remove rule 20000 above, which accepts all ICMP packets, and then choose which types of ICMP packets to allow. Some ICMP types such as those for message redirection and router solicitation are not typically needed. The following ICMP types are frequently judged necessary for network operation, and all other ICMP types are then denied:

```
# to allow destination unreachable messages
add 20001 allow icmp from any to any icmptypes 3
# to allow source quench / congestion control messages
add 20002 allow icmp from any to any icmptypes 4
# Allow ping responses (echo replies) in
add 20004 allow icmp from any to any icmptypes 0 in
# Allow "time exceeded" responses -- lets traceroute work
add 20005 allow icmp from any to any icmptypes 11 in
```

Removing rule 20000 and adding the rules above effectively enables Stealth Mode, since ICMP message of type 8 are implicitly denied (since they are not accepted). However, it may be necessary to allow ping responses to other systems on the local network but not from elsewhere. To do so, add a rule as follows, substituting your network/netmask for a.b.c.d/nm:

```
add 20010 allow icmp from a.b.c.d/nm to any icmptypes 8 in
```

Note: If Stealth Mode is enabled using the Security preference pane, the rule here will take precedence because has a lower number (20010) than the system applies for Stealth Mode (33000).

Packet fragmentation can be normal in some network environments. However, if your network environment should not result in packet fragmentation, then fragmented packets may be a sign of abnormal activity. The following rule will drop any fragmented packets:

```
add 700 deny log ip from any to any frag
```

Configuring the System to Load the IPFW Ruleset

The system must be configured to automatically load your IPFW ruleset in /etc/ipfw.conf at startup.

To do so, create the file /Library/LaunchDaemons/ipfw.plist so that it reads as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Label</key>
    <string>ipfw</string>
  <key>Program</key>
    <string>/sbin/ipfw</string>
  <key>ProgramArguments</key>
    <array>
      <string>/sbin/ipfw</string>
      <string>/etc/ipfw.conf</string>
    </array>
  <key>RunAtLoad</key>
    <true />
</dict>
</plist>
```

On the next reboot, the IPFW rules in /etc/ipfw.conf will be loaded automatically.

Understanding Passwords and Authentication

A Appendix

Use this appendix to learn the different types of passwords and how they authenticate users.

Passwords are a common method for authenticating. There are several types of services that use passwords to verify the identity of users.

Password Types

Each user account has a password type that determines how the user account is authenticated. In a local directory domain, the standard password type is shadow password. On a server upgraded from Mac OS X Server v10.3, user accounts in the local directory domain can also have an Open Directory password type.

For user accounts in the LDAP directory of Leopard Server, the standard password type is Open Directory. User accounts in the LDAP directory can also have a password type of crypt password.

Authentication and Authorization

Services such as the login window and Apple file service request user authentication from Open Directory. Authentication is part of the process by which a service determines whether it should grant a user access to a resource. Usually this process also requires authorization.

Authentication proves a user's identity, and authorization determines what the authenticated user is permitted to do. A user typically authenticates by providing a valid name and password. A service can then authorize the authenticated user to access specific resources. For example, File service authorizes full access to folders and files that an authenticated user owns.

You experience authentication and authorization when you use a credit card. The merchant authenticates you by comparing your signature on the sales slip to the signature on your credit card. Then the merchant submits your authorized credit card account number to the bank, which authorizes payment based on your account balance and credit limit.

Open Directory authenticates user accounts, and service access control lists (SACLs) authorize use of services. If Open Directory authenticates you, the SACL for login window determines whether you can log in, the SACL for Apple Filing Protocol (AFP) service determines whether you can connect for file service, and so on.

Some services also determine whether a user can access specific resources. This authorization can require retrieving other user account information from the directory domain. For example, AFP service needs the user ID and group membership information to determine which folders and files the user can read and write to.

Open Directory Passwords

When a user's account has a password type of Open Directory, the user can be authenticated by Kerberos or the Open Directory Password Server. Kerberos is a network authentication system that uses credentials issued by a trusted server. Open Directory Password Server supports traditional password authentication methods that some clients of network services require.

Kerberos and Open Directory Password Server do not store the password in the user's account. Kerberos and Open Directory Password Server store passwords in secure databases apart from the directory domain, and passwords can never be read. Passwords can only be set and verified.

Malicious users might attempt to log in over the network hoping to gain access to Kerberos and Open Directory Password Server. Open Directory logs can alert you to unsuccessful login attempts.

User accounts in the following directory domains can have Open Directory passwords:

- The LDAP directory of Leopard Server
- The local directory domain of Leopard Server

Note: Open Directory passwords can't be used to log in to Mac OS X v10.1 or earlier. Users who log in using the login window of Mac OS X v10.1 or earlier must be configured to use crypt passwords. The password type doesn't matter for other services. For example, a user of Mac OS X v10.1 could authenticate for Apple file service with an Open Directory password.

Shadow Passwords

Shadow passwords support the same traditional authentication methods as Open Directory Password Server. These authentication methods are used to send shadow passwords over the network in a scrambled form, or *hash*.

A shadow password is stored as several hashes in a file on the same computer as the directory domain where the user account resides. Because the password is not stored in the user account, the password is not easy to capture over the network. Each user's shadow password is stored in a separate file, named a *shadow password file*, and these files are protected so they can be read only by the root user account.

User accounts stored in a computer's local directory domain are the only ones that can have a shadow password. User accounts that are stored in a shared directory can't have a shadow password.

Shadow passwords also provide cached authentication for mobile user accounts. For more information about mobile user accounts, see *User Management*.

Crypt Passwords

A crypt password is stored in a hash in the user account record. This strategy, historically named *basic authentication*, is most compatible with software that needs to access user records directly. For example, Mac OS X v10.1 or earlier expect to find a crypt password stored in the user account.

Crypt authentication supports a maximum password length of eight bytes (eight ASCII characters). If a longer password is entered in a user account, only the first eight bytes are used for crypt password validation. Shadow passwords and Open Directory passwords are not subject to this length limit.

For secure transmission of passwords over a network, crypt supports the DHX authentication method.

Offline Attacks on Passwords

Because crypt passwords are stored in user accounts, they are subject to cracking. User accounts in a shared directory domain are accessible on the network. Anyone on the network who has Workgroup Manager or knows how to use command-line tools can read the contents of user accounts, including the passwords stored in them.

Open Directory passwords and shadow passwords aren't stored in user accounts, so these passwords can't be read from directory domains.

A malicious attacker could use Workgroup Manager or UNIX commands to copy user records to a file. The attacker can transport this file to a system and use various techniques to decode crypt passwords stored in the user records. After decoding a crypt password, the attacker can log in unnoticed with a legitimate user name and crypt password.

This form of attack is known as an offline attack, because it does not require successive login attempts to gain access to a system.

Shadow passwords and Open Directory passwords are far less susceptible to offline attacks because they are not stored in user records. Shadow passwords are stored in separate files that can be read only by someone who knows the password of the root user.

Open Directory passwords are stored securely in the Kerberos KDC and in the Open Directory Password Server database. A user's Open Directory password can't be read by other users, not even by a user with administrator rights for Open Directory authentication. (This administrator can change only Open Directory passwords and password policies.)

Password Guidelines

Many applications and services require that you create passwords to authenticate. Leopard includes applications that help create complex passwords (Password Assistant), and securely store your passwords (Keychain Access).

Leopard supports passwords that contain UTF-8 characters or any NUL-terminated byte sequence.

Creating Complex Passwords

Use the following tips to create complex passwords:

- Use a mixture of alphabetic (upper and lower case), numeric, and special characters (such as ! and @).
- Don't use words or combinations of words found in a dictionary of any language. Also, don't use names or anything else that is intelligible.
- Create a password of at least twelve characters. Longer passwords are generally more secure than shorter passwords.
- Create as random a password as possible.

You can use Password Assistant to verify the complexity of your password.

Using an Algorithm to Create a Complex Password

Consider creating an algorithm to make a complex (but memorable) password. Using an algorithm can increase the randomness of your password. Additionally, instead of needing to remember a complex password, you must remember only the algorithm.

The following example shows one possible algorithm for creating a complex password. Instead of using this algorithm, create your own or modify this one.

To create an algorithm for creating a complex password:

1. Choose your favorite phrase or saying.

 In this example, we'll use:

 Four score and seven years ago our fathers brought forth

 Ideally you should choose a phrase of at least eight words.

2. Reduce your favorite phrase to an acronym by keeping only the first letter of each word.

 The sample phrase becomes:

 Fsasyaofbf

3. Replace a letter with a number.

 If we replace "F" and the last "f" (from "four" and "forth") with "4", and "s" (from "seven") with "7," the sample phrase becomes:

 4sa7yaofb4

4. Add special characters.

 If we add "$" after "4," and "&" after "7," the sample phrase becomes:

 4$sa7&yaofb4$

5. Make some letters uppercase.

 If we convert all vowels to uppercase, the sample phrase becomes:

 4$sA7&yAOfb4$

Safely Storing Your Password

If you store your password or the algorithm used to make your password in a safe place, you can create more complex passwords without the fear of being unable to recover forgotten passwords.

When storing passwords, make sure your storage location is safe, unknown, and inaccessible to intruders. Consider storing your passwords in a sealed envelope inside a locked container. Alternatively, you can store your passwords in your wallet. By keeping your passwords in your wallet, you keep passwords in a safe location that is also convenient.

It is recommended not to store your password anywhere near your computer.

When writing down your password, take the following precautions:

- Don't identify the password as being a password.
- Don't include account information on the same piece of paper.
- Add some false characters or misinformation to the written password in a way that you remember. Make the written password different from the real password.
- Never record a password online, and never send a password to another person through email.

You can use Keychain Access to store your more complex, longer passwords. You'll still need a password to unlock Keychain Access so you can view and use these passwords.

Because Keychain Access requires that you authenticate to unlock keychains, it is convenient for you and inaccessible to intruders. Store the Keychain Access password in a safe location. For more information, see "Storing Credentials in Keychains" on page 107.

Password Maintenance

After you create a good password and store it in a safe location, do the following to make sure your password remains secure:

- Never tell anyone your password. If you tell someone your password, immediately change your password.
- Change your password frequently, and when you think your password has been compromised. If your account is compromised, notify authorities and close the account.
- Be aware of when trusted applications ask for your password. Malicious applications can mimic a trusted application and ask you for your password when you're not expecting it.
- Don't reuse the same password for multiple accounts. If you do, an intruder who compromises your password can use the password for all of those accounts.
- Don't enter password-related hints in "password hint" fields. By providing a hint, you compromise the integrity of your password.
- Don't access your account on public computers or other computers that you don't trust. Malicious computers can record your keystrokes.
- Don't enter your password in front of other people.

Authentication Services

Open Directory offers options for authenticating users whose accounts are stored in directory domains on Leopard Server, including Kerberos and traditional authentication methods that network services require.

Open Directory can authenticate users by:

- Using Kerberos authentication for single sign-on.
- Using traditional authentication methods and a password stored securely in the Open Directory Password Server database.
- Using traditional authentication methods and a shadow password stored in a secure shadow password file for each user.
- Using a crypt password stored directly in the user's account, for backward compatibility with legacy systems.
- Using a non-Apple LDAP server for LDAP bind authentication.

In addition, Open Directory lets you set up a password policy for all users as well as specific password policies for each user, such as automatic password expiration and minimum password length. (Password policies do not apply to administrators, crypt password authentication, or LDAP bind authentication.)

Determining Which Authentication Option to Use

To authenticate a user, Open Directory must determine which authentication option to use—Kerberos, Open Directory Password Server, shadow password, or crypt password. The user's account contains information that specifies which authentication option to use. This information is the *authentication authority attribute*.

Open Directory uses the name provided by the user to locate the user's account in the directory domain. Then Open Directory consults the authentication authority attribute in the user's account and learns which authentication option to use.

You can change a user's authentication authority attribute by changing the password type in the Advanced pane of Workgroup Manager, as shown in the following table.

Password type	Authentication authority	Attribute in user record
Open Directory	Open Directory Password Server and Kerberos[1]	Either or both: • ;ApplePasswordServer; • ;Kerberosv5;
Shadow password	Password file for each user, readable only by the root user account	Either: • ;ShadowHash;[2] • ;ShadowHash;*<list of enabled authentication methods>*
Crypt password	Encoded password in user record	Either: • ;basic; • no attribute at all

[1] User accounts from Mac OS X Server v10.2 must be reset to include the Kerberos authentication authority attribute.
[2] If the attribute in the user record is ;ShadowHash; without a list of enabled authentication methods, default authentication methods are enabled. The list of default authentication methods is different for Leopard Server and Leopard.

The authentication authority attribute can specify multiple authentication options. For example, a user account with an Open Directory password type normally has an authentication authority attribute that specifies Kerberos and Open Directory Password Server.

A user account doesn't need to include an authentication authority attribute. If a user's account contains no authentication authority attribute, Leopard Server assumes a crypt password is stored in the user's account. For example, user accounts created using Mac OS X v10.1 or earlier contain a crypt password but not an authentication authority attribute.

Password Policies

Open Directory enforces password policies for users whose password type is Open Directory or shadow password. For example, a user's password policy can specify a password expiration interval. If the user is logging in and Open Directory determines that the user's password has expired, the user must replace the expired password. Then Open Directory can authenticate the user.

Password policies can disable a user account on a specified date, after a number of days, after a period of inactivity, or after a number of failed login attempts. Password policies can also require passwords to be a minimum length, contain at least one letter, contain at least one number, differ from the account name, differ from recent passwords, or be changed periodically.

The password policy for a mobile user account applies when the account is used while disconnected from the network and while connected to the network. A mobile user account's password policy is cached for use while offline. For more information about mobile user accounts, see *User Management*.

Password policies do not affect administrator accounts. Administrators are exempt from password policies because they can change the policies at will. In addition, enforcing password policies on administrators could subject them to denial-of-service attacks.

Kerberos and Open Directory Password Server maintain password policies separately. An Open Directory server synchronizes the Kerberos password policy rules with Open Directory Password Server password policy rules.

Single Sign-On Authentication

Leopard Server uses Kerberos for single sign-on authentication, which relieves users from entering a name and password separately for every service. With single sign-on, a user always enters a name and password in the login window. Thereafter, the user does not need to enter a name and password for Apple file service, Mail service, or other services that use Kerberos authentication.

To take advantage of single sign-on, users and services must be Kerberized—configured for Kerberos authentication—and use the same Kerberos Key Distribution Center (KDC) server.

User accounts that reside in an LDAP directory of Leopard Server and have a password type of Open Directory use the server's built-in KDC. These user accounts are configured for Kerberos and single sign-on. The server's Kerberized services use the server's built-in KDC and are configured for single sign-on.

This Mac OS X Server KDC can also authenticate users for services provided by other servers. Having more servers with Leopard Server use the Mac OS X Server KDC requires only minimal configuration.

Kerberos Authentication

Kerberos was developed at MIT to provide secure authentication and communication over open networks like the Internet. It's named for the three-headed dog that guarded the entrance to the underworld of Greek mythology.

Kerberos provides proof of identity for two parties. It enables you to prove who you are to network services you want to use. It also proves to your applications that network services are genuine, not spoofed.

Like other authentication systems, Kerberos does not provide authorization. Each network service determines what you are permitted to do based on your proven identity.

Kerberos permits a client and a server to identify each other much more securely than typical challenge-response password authentication methods. Kerberos also provides a single sign-on environment where users authenticate only once a day, week, or other period of time, easing authentication frequency.

Leopard Server offers integrated Kerberos support that virtually anyone can deploy. Kerberos deployment is so automatic that users and administrators might not realize it's deployed.

Mac OS X v10.3 and later use Kerberos when someone logs in using an account set for Open Directory authentication. It is the default setting for user accounts in the Mac OS X Server LDAP directory. Other services provided by the LDAP directory server, such as AFP and Mail service, also use Kerberos.

If your network has other servers with Leopard Server, joining them to the Kerberos server is easy, and most of their services use Kerberos automatically.

Alternatively, if your network has a Kerberos system such as Microsoft Active Directory, you can set up your Leopard Server and Leopard computers to use it for authentication.

Leopard Server and Leopard or later support Kerberos v5. Leopard Server and Leopard do not support Kerberos v4.

Smart Card Authentication

Smart cards enable you to carry your digital certificates with you. Leopard allows you to use your smart card when an authentication dialog is presented.

This robust, two-factor authentication mechanism complies with Department of Defense Common Access Card, U.S. PIV, Belgium National Identification Card, Japanese government PKI, and Java Card 2.1 standards. Similar to an ATM card and a PIN code, two-factor authentication relies on something you have and something you know. If your smart card is lost or stolen, it cannot be used unless your PIN is also known.

Security Checklist

This appendix contains a checklist of recommended steps required to secure Leopard Server.

This appendix contains action item checklists ordered by chapter.

You can customize these checklists to suit your needs. For example, you can mark the completion status of action items in the "Completed?" column. If you deviate from the suggested action item, you can use the "Notes" column to justify or clarify your decision.

Installation Action Items

For details, see Chapter 2, "Installing Leopard Server," on page 36.

Action Item	Completed?	Notes
Securely erase the Mac OS X install partition before installation		
Disable the Open Firmware password before installation		
Install Leopard Server using Mac OS Extended disk formatting		
Do not install unnecessary packages		
Do not transfer confidential information in Server Assistant		
Do not connect to the Internet		
Create administrator accounts with difficult-to-guess names		
Create complex passwords for administrator accounts		

Action Item	Completed?	Notes
Do not enter a password-related hint; instead, enter help desk contact information		
Enter correct time settings		
Use an internal Software Update server		
Update system software using verified packages		
Repair disk permissions after installing software or software updates		

Hardware and Core Leopard Server Action Items

For details, see Chapter 3, "Protecting System Hardware," on page 75.

Action Item	Completed?	Notes
Restrict access to rooms that have computers		
Store computers in locked or secure containers when not in use		
Use a password protected screensaver		

Global Settings for Leopard Server Action Items

For details, see Chapter 4, "Securing Global System Settings," on page 86.

Action Item	Completed?	Notes
Require an Open Firmware or EFI password		
Create an access warning for the login window		
Create an access warning for the command line		
Disable fast user switching with non-trusted users or when multiple users access local accounts		

Account Configuration Action Items

For details, see Chapter 5, "Securing Local Server Accounts," on page 94.

Action Item	Completed?	Notes
Create an administrator account and a standard account for each administrator		
Create a standard or a managed account for each nonadministrator		
Set parental controls for managed accounts		
Restrict the distribution and use of administrator accounts		
Modify the /etc/authorization file to secure directory domain access		
Disable su		
Disable root account		
Restrict sudo users to only being able to access required commands		
Set a strong password policy		
Use Password Assistant to generate complex passwords		
Authenticate using a smart card, token, or biometric device		
Secure the login keychain		
Secure keychain items		
Create specialized keychains for different purposes		
Use a portable drive to store keychains		

System Software Action Items

Chapter 5, "Securing Local Server Accounts," describes how to secure system preferences. Every system preference with security-related configuration settings has its own action item checklist.

MobileMe Preferences Action Items

For details, see "Securing MobileMe Preferences" on page 114.

Action Item	Completed?	Notes
Disable all Sync options		
Disable iDisk Syncing		
Enable Public Folder password protection		
Do not register computers for synchronization		

Accounts Preferences Action Items

For details, see "Securing Accounts Preferences" on page 116.

Action Item	Completed?	Notes
Change the initial password for the system administrator account		
Disable automatic login		
Display the login window as name and password		
Disable "Show password hints"		
Disable "Enable fast user switching"		
Disable "Show the Restart, Sleep, and Shut Down buttons"		

Appearance Preferences Action Items

For details, see "Securing Appearance Preferences" on page 119.

Action Item	Completed?	Notes
Do not display recent applications		
Do not display recent documents		
Do not display recent servers		

Bluetooth Preferences Action Items

For details, see "Securing Bluetooth Preferences" on page 120.

Action Item	Completed?	Notes
Disable Bluetooth for each user account in System Preferences		
Remove privileges to modify Bluetooth System Preferences		

CDs & DVDs Preferences Actions Items

For details, see "Securing CDs & DVDs Preferences" on page 121.

Action Item	Completed?	Notes
Disable automatic actions for blank CDs for each user account		
Disable automatic actions for blank DVDs for each user account		
Disable automatic actions for music CDs for each user account		
Disable automatic actions for picture CDs for each user account		
Disable automatic actions for video DVDs for each user account		
Remove privileges to modify CDs & DVDs System Preferences		

Exposé & Spaces Preferences Action Items

For details, see "Securing Exposé & Spaces Preferences" on page 130

Action Item	Completed?	Notes
Disable Dashboard		

Date & Time Preferences Action Items

For details, see "Securing Date & Time Preferences" on page 123.

Action Item	Completed?	Notes
Set a correct date and time		
Use a secure internal NTP server for automatic date and time setting		

Desktop & Screen Saver Preferences Action Items

For details, see "Securing Desktop & Screen Saver Preferences" on page 125.

Action Item	Completed?	Notes
Set a short inactivity interval for the screen saver		
Set a screen corner to Start Screen Saver for each user account		
Do not set a screen corner to Disable Screen Saver for each user account		
Remove privileges to modify Dashboard and Exposé System Preferences		

Display Preferences Action Items

For details, see "Securing Display Preferences" on page 127.

Action Item	Completed?	Notes
Disable display mirroring		

Dock Preferences Action Items

For details, see "Securing Dock Preferences" on page 127.

Action Item	Completed?	Notes
Set the dock to hide when not in use		

Energy Saver Preferences Action Items

For details, see "Securing Energy Saver Preferences" on page 128.

Action Item	Completed?	Notes
Disable sleeping the computer for all power settings		
Enable sleeping the display for all power settings		
Enable sleeping the hard disk for all power settings		
Disable "Wake when the modem detects a ring" for all power settings		
Disable "Wake for Ethernet network administrator access" for power adapter settings		

Action Item	Completed?	Notes
Disable "Restart automatically after a power failure" for all power settings		
Disable "Restart automatically if the computer freezes" for all power settings		

Keyboard and Mouse Preferences Action Items

For details, see "Securing Keyboard & Mouse Preferences" on page 132.

Action Item	Completed?	Notes
Turn off Bluetooth		

Network Preferences Action Items

For details, see "Securing Network Preferences" on page 132.

Action Item	Completed?	Notes
Disable unused hardware devices		
Disable IPv6		

Print & Fax Preferences Action Items

For details, see "Securing Print & Fax Preferences" on page 135.

Action Item	Completed?	Notes
Use printers in secure locations only		
Disable printer sharing		
Disable print browsing		
Disable receiving faxes		
Disable sending faxes		

QuickTime Preferences Action Items

For details, see "Securing QuickTime Preferences" on page 137.

Action Item	Completed?	Notes
Disable "Save movies in disk cache"		
Do not install third-party QuickTime software		

Security Preferences Action Items

For details, see "Securing Security Preferences" on page 138.

Action Item	Completed?	Notes
Require a password to wake the computer from sleep or screen saver for each account		

Sharing Preferences Action Items

For details, see "Securing Sharing Preferences" on page 139.

Action Item	Completed?	Notes
Disable Remote Login		
Disable Apple Remote Desktop		
Disable Remote Apple Events		
Rename your computer to a name that does not indicate the purpose of the computer		

Software Update Preferences Action Items

For details, see "Securing Software Update Preferences" on page 141.

Action Item	Completed?	Notes
Set "Check for updates" according to policy		
Disable "Download important updates in the background"		
Manually update using installer packages		
Transfer installer packages from a test computer		
Verify installer packages before installing		

Sound Preferences Action Items

For details, see "Securing Sound Preferences" on page 142.

Action Item	Completed?	Notes
Minimize input volume for the internal microphone		
Minimize input volume for the audio line-in port		

Speech Preferences Action Items

For details, see "Securing Speech Preferences" on page 143.

Action Item	Completed?	Notes
Enable speech recognition in a secure environment only		
Use headphones if you enable text to speech		

Spotlight Preferences Action Items

For details, see "Securing Spotlight Preferences" on page 145.

Action Item	Completed?	Notes
Prevent Spotlight from searching confidential folders		

Startup Disk Preferences Action Items

For details, see "Securing Startup Disk Preferences" on page 147.

Action Item	Completed?	Notes
Carefully choose the startup volume		

Time Machine Preferences Action Items

For details, see "Securing Time Machine Preferences" on page 149.

Action Item	Completed?	Notes
Turn Time Machine on		
Select a safe location to store backups in		

Data Maintenance and Encryption Action Items

For details, see Chapter 7, "Securing Data and Using Encryption," on page 151.

Action Item	Completed?	Notes
Set global permissions using POSIX or ACLs		
Strip setuid bits		
Secure home directory permissions		
Enable FileVault for every user		
Encrypt portable files		

Action Item	Completed?	Notes
Set global umask by changing NSUmask settings		
Mandate secure erasing of files		
Mandate secret erasing of partitions		
Mandate securely erasing free space		

Account Policies Action Items

Chapter 11, "Securing Accounts and Share Points," describes how to set up and manage account policies and user accounts, as well as how to configure settings and preferences for clients. Each topic with security-related configuration settings has its own action item checklist.

Share Points Action Items

For details, see Chapter , "Configuring Share Points,".

Action Item	Completed?	Notes
Enable SSL in Workgroup Manager		
Disable unused share points		
Disable unused sharing protocols		
Restrict share point access		

Account Configuration Action Items

For details, see "Securing Accounts" on page 185.

Action Item	Completed?	Notes
Disallow simultaneous login		
Use an Open Directory password instead of a crypt password		
Enter a disk quota		
Use POP or IMAP for mail, not both		
Use POSIX or ACL permissions to determine group account access		
Restrict access to specific groups by assigning computers to a list		

Action Item	Completed?	Notes
If accounts are stored in a network domain, disable local accounts		
Specify a time interval to update the preferences cache		

Applications Preferences Action Items

For details, see "Managing Applications Preferences" on page 300.

Action Item	Completed?	Notes
Create a list of approved applications that users can open		
Deselect "User can also open all applications on local volumes"		
Deselect "Allow approved applications to launch non-approved applications"		
Deselect "Allow UNIX tools to run"		

Dock Preferences Action Items

For details, see "Managing Dock Preferences" on page 306.

Action Item	Completed?	Notes
Modify the Applications list to include required applications		
Modify the Documents and Folders list to include required documents and folders		
Deselect '"Merge with user's Dock"		
Deselect "My Applications"		
Deselect "Documents"		
Deselect "Network Home"		
Select "Automatically hide and show the Dock"		

Energy Saver Preferences Action Items

For details, see "Managing Energy Saver Preferences" on page 307.

Action Item	Completed?	Notes
Disable sleeping the computer for all power settings		
Deselect "Start up the computer"		

Finder Preferences Action Items

For details, see "Managing Finder Preferences" on page 308.

Action Item	Completed?	Notes
Select "Use normal finder"		
Deselect "Hard Disks"		
Deselect "Removable media (such as CDs)"		
Deselect "Connected Servers"		
Select "Always show file extensions"		
Deselect "Connect to Server"		
Deselect "Go to iDisk"		
Deselect "Go to Folder"		
Deselect "Eject"		
Deselect "Burn Disk"		
Deselect "Restart"		
Deselect "Shut Down"		

Login Preferences Action Items

For details, see"Managing Login Preferences" on page 310.

Action Item	Completed?	Notes
Deselect "Add network home share point"		
Deselect "User may add and remove additional items"		
Deselect "User may press Shift to keep items from opening"		
Do not allow login or logout scripts		
Do not allow LoginHook or LogoutHook scripts		

Action Item	Completed?	Notes
Enter help desk information as the login message		
Display the login window as name and password text fields		
Do not allow Restart or Shut Down buttons to show in the Login Window		
Do not allow password hints		
Deselect "Auto Login Client Setting"		
Deselect "Allow users to log in using '>console.'"		
Deselect "Enable Fast User Switching"		
Deselect "Log out users after # minutes of activity"		

Media Access Preferences Action Items

For details, see "Managing Media Access Preferences" on page 313.

Action Item	Completed?	Notes
Disable unnecessary media		
Deselect "Allow for CDs"		
Deselect "Allow for CD-ROMs"		
Deselect "Allow for DVDs"		
Deselect "Allow for Recordable Disks"		
Deselect "Allow for Internal Disks"		
Deselect "Allow for External Disks"		
Select "Eject all removable media at logout"		

Mobility Preferences Action Items

For details, see "Managing Mobility Preferences" on page 314.

Action Item	Completed?	Notes
Disable mobile account on insecure or infrequently accessed computers		
Use FileVault on every computer with portable home folders		
Deselect "Synchronize account for offline use"		

Network Preferences Action Items

For details, see "Managing Network Preferences" on page 316.

Action Item	Completed?	Notes
Use your organization-controlled proxy servers		
Bypass trusted hosts and domains		
Deselect "Use Passive FTP Mode (PASV)"		

Printing Preferences Action Items

For details, see "Managing Printing Preferences" on page 321.

Action Item	Completed?	Notes
Reduce access to printers		
Deselect "Allow user to modify the printer list"		
Deselect "Allow printers that connect directly to user's computer"		
If selecting "Allow printers that connect directly to user's computer", then select "Require an administrator password"		
Select a printer and select "Require an administrator password"		

Software Update Preferences Action Items

For details, see "Managing Software Update Preferences" on page 322.

Action Item	Completed?	Notes
Designate an internal server to control software updates		

Access to System Preferences Action Items

For details, see "Managing Access to System Preferences" on page 323.

Action Item	Completed?	Notes
Select "Appearance" to appear in the System Preferences preferences		
Select "Dashboard & Exposé" to appear in the System Preferences preferences		
Select "Displays" to appear in the System Preferences preferences		
Select "Dock" to appear in the System Preferences preferences		
Select "Keyboard & Mouse" to appear in the System Preferences preferences		
Select "Security" to appear in the System Preferences preferences		
Select "Universal" to appear in the System Preferences preferences		
Disable widgets for network managed users		

Universal Access Preferences Action Items

For details, see "Managing Universal Access Preferences" on page 324.

Action Item	Completed?	Notes
Deselect "Turn on Zoom"		
Set Sticky Keys to Off		
Deselect "Show pressed keys on screen"		

Certificates Action Items

For details, see "Managing Certificates" on page 189.

Action Item	Completed?	Notes
Obtain certificates to use with SSL-enabled services		
Create a CA to issue certificates		
Create an SSL certificate for distribution		
Create the files and folders needed by SSL		
Export certificate to client computers		

General Protocols and Service Access Action Items

For details, see "Setting General Protocols and Access to Services" on page 201.

Action Item	Completed?	Notes
Configure NTP to use an internal time server		
Disable SNMP		
Enable SSH		
Do not use "server" or your name to identify the server		
Set a correct date and time		
Use a secure internal NTP server for automatic date and time setting		
Use Certificate Manager to create, use, and maintain identities for SSL-enabled services		
Use SACL to restrict access to AFP, FTP, and Windows file services		

Remote Access Services Action Items

For details, see "Securing Remote Access Services" on page 207.

Action Item	Completed?	Notes
Disable root login using SSH		
Modify the /private/etc/sshd_config file to further secure SSH		
Generate identity key pairs for login authentication		
Configure access for using SSH through Server Admin using SACLs		
Use SFTP instead of FTP		
Disable VPN services		
If using VPN services, enable either or both L2TP and PPTP		
To use SecurID authentication, edit the VPN configuration file manually		
Configure an access warning banner		
Disable Apple Remote Desktop		
Encrypt Observe and Control traffic by setting "Encrypt all network data"		
Encrypt network data during file copy and package installation by setting "Encrypt transfers when using Install Packages"		
Disable Remote Apple Events		

Network and Host Access Services Action Items

"Securing Network and Host Access Services" on page 221 describes configuration information to secure your network services. Several services are provided to maintain your network. Each service with security-related configuration settings has its own action item checklist.

IPv6 Protocol Action Items

For details, see "Using IPv6 Protocol" on page 221.

Action Item	Completed?	Notes
Enable IPv6		
Configure IPv6 manually or automatically		

DHCP Service Action Items

For details, see "Securing DHCP Service" on page 222.

Action Item	Completed?	Notes
Disable the DHCP service if not required		
If using DHCP, disable DNS, LDAP, and WINS		
Assign static IP addresses		

DNS Service Action Items

For details, see "Securing DNS Service" on page 225.

Action Item	Completed?	Notes
Disable the DNS service		
Allow only one system to act as the DNS server		
Allow recursive queries and zone transfers only from trusted clients, not from external networks.		
Update and audit DNS regularly		
Specify which IP addresses are allowed to request zone transfers		
Configure BIND to respond with something other than the current version		
Limit or disable DNS recursion		

Firewall Service Action Items

For details, see "Securing Firewall Service" on page 231.

Action Item	Completed?	Notes
Create IP address groups		
Configure firewall rules for groups and services		
Configure advanced rules for groups and services		
Enable stealth mode		
Set up logging		

NAT Service Action Items

For details, see "Securing NAT Service" on page 237.

Action Item	Completed?	Notes
Disable NAT service if not required		
Configure NAT service		
If necessary, forward incoming traffic to an IP address		

Bonjour Service Action Items

For details, see "Securing Bonjour Service" on page 240.

Action Item	Completed?	Notes
Disable Bonjour unless required		
Disable unused services that should not be discovered through Bonjour		

Collaboration Services Action Items

For details, see "Securing iCal Service" on page 242 and "Securing iChat Service" on page 245.

Action Item	Completed?	Notes
Disable iCal service		
Disable iChat service		
If using iChat service, designate domain names to use		

Action Item	Completed?	Notes
Designate a certificate to use		
Monitor communication using iChat service logs		

Mail Service Action Items

For details, see "Securing Mail Service" on page 253.

Action Item	Completed?	Notes
Turn off support for any protocol that is not required		
Use different systems for providing outgoing and incoming mail service		
Enable SSL for the mail server		
Create and install a signed mail certificate for outgoing and incoming mail service protocols		
Use the "require" setting in the SSL support options (recommended)		
Configure SMTP authentication requirements to reduce junk mail		
Create a list of approved host servers to relay mail		
Enable junk mail filtering		
Enable virus filtering		
Update the virus database at least twice a day		
Set up a problem report account		
Disable the SMTP banner		

File Services Action Items

"Securing File Services" on page 274 describes configuring file sharing services. Each type of file sharing service with security-related configuration settings has its own action item checklist.

Action Item	Completed?	Notes
Disable file sharing services if not required		
Use as few protocols as possible		
Use AFP		
Disable FTP		
Disable NFS		
Disable SMB		

AFP File Sharing Service Action Items

For details, see "Configuring AFP File Sharing Service" on page 278.

Action Item	Completed?	Notes
Disable Bonjour registration		
Disable browsing with AppleTalk		
Disable Guest access		
Disable administrator to masquerade as another user		
Enter "1" for Guest Connections		
Enable access log		
Set frequency of archiving		
Implement settings for idle user		

FTP File Sharing Service Action Items

For details, see "Configuring FTP File Sharing Service" on page 280.

Action Item	Completed?	Notes
If authentication is possible, use SFTP instead of FTP		
Disconnect client after 1 login failure		
Enter a mail address set up to handle FTP administration		
Select Kerberos for access authentication		
Allow a maximum of 1 authenticated user		

Action Item	Completed?	Notes
Enable anonymous access and designate the number of anonymous users		
Disable MacBinary and disk image autoconversion		
Enable "Show Welcome Message"		
Enable "Show Banner Message"		
Log all login attempts		
Set "Authenticated users see:" to FTP root and Share Points		
Designate files to share with anonymous users		
Configure the /Library/FTPServer/Configuration/ftpaccess		

NFS File Sharing Service Action Items

For details, see "Configuring NFS File Sharing Service" on page 282.

Action Item	Completed?	Notes
Use NFS only on a secure LAN or when Apple and Windows file sharing systems are unavailable		
Restrict an NFS share point to those systems that require it		
Make the list of export options as restrictive as possible		

SMB Action Items

For details, see "Configuring SMB File Sharing Service" on page 283.

Action Item	Completed?	Notes
Do not allow guest access		
Enter the maximum number of clients connections expected		
Set "Log Detail" to at least medium		
Deselect Workgroup Master Browser and Domain Master Browser services		
Turn off WINS registration		

Web Service Action Items

For details, see "Securing Web Service" on page 285.

Action Item	Completed?	Notes
Disable Web service if not required		
Disable web modules if not required		
Disable web options if not required		
Create or obtain signed certificates for each domain name		
Enable SSL for Web service		
If WebDAV is enabled, assign access privileges for the sites and web folders		
Do not allow web content files and folders to be writable by world		
Configure a realm to allow user access to websites		
Allow users to access blogs through an SSL enabled site		

Client Configuration Management Services Action Items

For details, see "Securing Client Configuration Management Services" on page 300.

Action Item	Completed?	Notes
Disable NetBoot and NetBoot disk images		
Use Server Admin to view NetBoot clients and the status of NetBoot service		

Directory Services Action Items

For details, see "Securing Directory Services" on page 333.

Action Item	Completed?	Notes
Configure Open Directory roles		
Configure Kerberos		

Action Item	Completed?	Notes
Set a server outside of directory domains as Standalone Server		
Enable SSL		
Set global password policies		
Set binding policies		
Set security policies for Open Directory		

Print Service Action Items

For details, see "Securing Print Service" on page 347.

Action Item	Completed?	Notes
Use Server Admin to manage print queues and configure settings		
Specify a default LPR queue		

Multimedia Services Action Items

For details, see "Securing Multimedia Services" on page 353.

Action Item	Completed?	Notes
User Server Admin to configure QTSS		
Use secure digest authentication to configure client access to streamed media files		

Grid and Cluster Computing Services Action Items

For details, see "Securing Grid and Cluster Computing Services" on page 363.

Action Item	Completed?	Notes
If possible, use a single sign-on password		
Always require authentication		
Enable Xgrid agent service		
Set a password for your Xgrid		
Enable Xgrid controller service		
Set a password for your Xgrid controller		

Action Item	Completed?	Notes
Set a password for the server acting as a grid agent		
Set a password for agents to join a grid and clients to submit jobs		

Validating System Integrity Action Items

For details, see "Maintaining System Integrity" on page 376.

Action Item	Completed?	Notes
Install and enable auditing tools		
Configure audit settings		
Configure log files		
Configure local system using syslog.conf		
Enable remote system logging		
Install file integrity tools		
Install antivirus tools		

Scripts

```
# ---------------------------------------------------------------------
# Protecting System Hardware
# ---------------------------------------------------------------------
# Securing Wi-Fi Hardware
# ----------------------
# Remove AppleAirport kernel extensions
srm -r /System/Library/Extensions/AppleAirPort.kext
srm -r /System/Library/Extensions/AppleAirPort2.kext
srm -r /System/Library/Extensions/AppleAirPortFW.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Removing BlueTooth Software
# ---------------------------
# Remove Bluetooth kernel extensions
srm -r /System/Library/Extensions/IOBluetoothFamily.kext
srm -r /System/Library/Extensions/IOBluetoothHIDDriver.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Removing IR Support Software
# ----------------------------
# Remove IR kernel extensions.
srm -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Removing Audio Recording Software
# ---------------------------------
# Remove Audio Recording kernel extensions
srm -r /System/Library/Extensions/AppleOnboardAudio.kext
srm -r /System/Library/Extensions/AppleUSBAudio.kext
srm -r /System/Library/Extensions/AppleDeviceTreeUpdater.kext
srm -r /System/Library/Extensions/IOAudioFamily.kext
srm -r /System/Library/Extensions/VirtualAudioDriver.kext
```

```
# Remove Extensions cache files
touch /System/Library/Extensions

# Removing Video Recording Software
# ---------------------------------
# Remove Video Recording kernel extensions.

# Remove external iSight camera.
srm -rf /System/Library/Extensions/Apple_iSight.kext

# Remove internal iSight camera.
srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/
     AppleUSBVideoSupport.kext

# Remove Extensions cache files.
touch /System/Library/Extensions

# Removing USB Support
# --------------------
# Remove USB kernel extensions
srm -r /System/Library/Extensions/IOUSBMassStorageClass.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Securing FireWire Hardware
# ------------------------------
# Remove FireWire kernel extensions
srm -r /System/Library/Extensions/IOFireWireSerialBusProtocolTransport.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Securing Global System Settings
# ---------------------------------------------------------------------------
# Configuring Open Firmware Settings
# ----------------------------------
# Secure startup by setting security-mode. Replace $mode-value with
# “command” or “full”.
nvram security-mode=”$mode-value”

# Verify security-mode setting.
nvram -p

# Enabling Access Warning for the Login Window
# --------------------------------
# Create a login window access warning.
defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText
     “Warning Text”
# You can also used the BannerSample project to create an access warning.
```

```
# ------------------------------------------------------------------
# Securing System Preferences
# ------------------------------------------------------------------
# Securing MobileMe Preferences
# -------------------------
# Disable Sync options.
defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer 1
# Disable iDisk Syncing.
defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool no

# Securing Accounts Preferences
# -----------------------------
# Change an account's password on a client system.
# Don't use this commands if other users are also logged in
sudo dscl /LDAPv3/127.0.0.1 passwd /Users/$User_name $Oldpass $Newpass

# Change an account's password on a server.
# Don't use this commands if other users are also logged in
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass

# Make sure there is no password hint set.
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint -
     int 0

# Set the login options to display name and password in the login window.
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool
     yes

# Disable Show the Restart, Sleep, and ShutDown Buttons.
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
     bool yes

# Disable fast user switching. This command does not prevent multiple users
# from being logged in.
defaults write /Library/Preferences/.GlobalPreferences
     MultipleSessionEnabled -bool NO

# Securing Appearance Preferences
# -------------------------------
# Disable display of recent applications.
defaults write com.apple.recentitems Applications -dict MaxAmount 0

# Securing Bluetooth Preferences
# ------------------------------
# Turn Bluetooth off
defaults write /Library/Preferences/com.apple.Bluetooth ControllerPowerState
     -int 0
```

```
# Securing CDs & DVDs Preferences
# ------------------------------
# Disable blank CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.cd.appeared -dict action 1

# Disable music CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.music.appeared -dict action 1

# Disable picture CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.picture.appeared -dict action 1

# Disable blank DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.dvd.appeared -dict action 1

# Disable video DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.dvd.video.appeared -dict action 1

# Securing Date & Time Preferences
# --------------------------------
# Set the NTP server.
cat >> /etc/ntp.conf << END server time.apple.com END

# Set the Date and Time.
systemsetup -settimezone $Time_Zone

# Disable NTPD if there is no trusted NTPD available.
launchctl unload -w org.ntp.ntpd.plist

# Securing Desktop & Screen Saver Preferences
# -------------------------------------------
# Set idle time for screen saver. XX is the idle time in seconds.
defaults -currentHost write com.apple.screensaver idleTime -int XX

# Set host corner to activate screen saver.
# wvous-bl-corner (bottom-left)
# wvous-br-corner(bottom-right)
# wvous-tl-corner (top-left)
# wvous-tr-corner (top-right)
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-corner
     -int 5

# Set modifier key to 0 wvous-corner_code-modifier
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
     modifier -int 0
```

```
# Securing Dock Preferences
# -------------------------
# Automatically hide and show Dock
defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Restart dock
killall -HUP Dock

# Securing Energy Saver Preferences
# ---------------------------------
# Disable computer sleep.
pmset -a sleep 0

# Enable hard drive sleep.
pmset -a disksleep $minutes

# Disable Wake for Ethernet network administrator access.
pmset -a womp 0

# Disable Restart automatically after power failure.
pmset -a autorestart 0

# Securing Exposé & Spaces Preferences
# ------------------------------------
# Disable dashboard.
$ sudo launchctl unload -w /System/Library/LaunchDaemons/
     com.apple.dashboard.advisory.fetch.plist

# Securing Keyboard & Mouse Preferences
# -------------------------------------
# Disable Bluetooth Devices to wake computer
defaults write /Library/Preferences/com.apple.Bluetooth.plist
     BluetoothSystemWakeEnable -bool 0

# Securing Network Preferences
# ----------------------------
# Disable unused hardware
# The interface value ($interface) can be AirPort, Bluetooth,
" "Built-in Ethernet", or "Built-in FireWire".
networksetup -setnetworkserviceenabled $interface off

# Securing Network Preferences
# ----------------------------
# Disable IPv6
# The interface value ($interface) can be AirPort, Bluetooth,
" "Built-in Ethernet", or "Built-in FireWire".
networksetup -setv6off $interface
```

```
# Securing Printer & Fax Preferences
# ---------------------------------
# Disable the receiving of faxes.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist

# Disable printer sharing.
cp /etc/cups/cupsd.conf $TEMP_FILE
if /usr/bin/grep "Port 631" /etc/cups/cupsd.conf
then
     /usr/bin/sed "/^Port 631.*/s//Listen localhost:631/g" $TEMP_FILE
     /etc/cups/cupsd.conf
else
     echo "Printer Sharing not on"
fi

# Disable printer browsing
Browsing Off
BrowseAllow none

# Securing Security Preferences
# -----------------------------
# Enable Require password to wake this computer from sleep or screen
# saver.
defaults -currentHost write com.apple.screensaver askForPassword -int 1

# Enable FileVault.
# To enable FileVault for new users, use this command.
/System/Library/CoreServices/ManagedClient.app/Contents/Resources/
     createmobileaccount

# Securing Sharing Preferences
# ----------------------------
# Change the computer name, where $host_name is the name of the computer.
# This command does not change the Bonjour host name.
systemsetup -setcomputername $host_name

# Change the Bonjour host name, where $Bon_host_name must not contain
# spaces or other non-DNS characters.
scutil --set LocalHostName $Bon_host_name

# Securing Software Updates Preferences
# -------------------------------------
# Disable check for updates and Download important updates automatically
softwareupdate --schedule off

# Securing Sound Preferences
# --------------------------
# Disable internal microphone or line-in.
# This command does not change the input volume for all input devices. It
# only sets the default input device volume to zero.
osascript -e “set volume input volume 0”
```

```
# Securing Speech Preferences
# ----------------------------
# Disable Speech Recognition
defaults write "com.apple.speech.recognition.AppleSpeechRecognition.prefs"
     StartSpeakableItems -bool false

# Disable Text to Speech settings
defaults write "com.apple.speech.synthesis.general.prefs"
     TalkingAlertsSpeakTextFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenNotificationAppActivationFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenUIUseSpeakingHotKeyFlag -bool false
defaults delete "com.apple.speech.synthesis.general.prefs"
     TimeAnnouncementPrefs

# Securing Spotlight Preferences
# ----------------------------
# Disable Spotlight for a volume and erase its current meta data. Where
# $volumename is the name of the volume.
$ mdutil -E -i off $volumename

# Securing Startup Disk Preferences
# ----------------------------
# Set startup disk
systemsetup -setstartupdisk $path

# Securing Time Machine Preferences
# --------------------------------
# Enable Time Machine
defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1

# ---------------------------------------------------------------------
# Using Disk Utility to Securely Erase Free Space
# ---------------------------------------------------------------------
# Overwrite a device with zeroes.
diskutil zeroDisk /dev/device

# Secure erase (7-pass) free space on a volume.
diskutil secureErase freespace 2 /dev/device

# Secure erase (7-pass) a volume.
diskutil secureErase 2 /dev/device

# Securing System Swap and Hibernation Storage
# ----------------------------
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
     UseEncryptedSwap -bool YES
```

```
# ------------------------------------------------------------------
# Setting General Protocols
# ------------------------------------------------------------------

# Disable NTP
# -----------
systemsetup -setusingnetworktime off

# Disable SNMP
# ------------
service org.net-snmp.snmpd stop

# Enable SSH
# ----------
service ssh start

# Remote Management (ARD)
# ---------------------------
# Disable Remote Management.
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
     Resources/kickstart -deactivate -stop

# Remote Apple Events (RAE)
# ---------------------------
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist

# Set SACL permissions for a service
# ----------------------------------
dseditgroup -o edit -a $USER -t user $SACL_GROUP

# Remote Apple Events (RAE)
# ---------------------------
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist

# ------------------------------------------------------------------
# Enabling IPv6
# ------------------------------------------------------------------

# Enable IPv6
# -------------------------------
networksetup -setv6on [networkservice]

# ------------------------------------------------------------------
# Securing DHCP Service
# ------------------------------------------------------------------

# Disable DHCP Service
# --------------------
serveradmin stop dhcp
```

```
# Configuring DHCP Services
# -------------------------
# Set a DHCP subnet's DNS, LDAP, and WINS parameters to no value
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:dhcp_domain_name_server:_array_index:0 = ""
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:dhcp_ldap_url:_array_index:0 = -empty_array
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:WINS_node_type =" NOT SET"

# ------------------------------------------------------------------------
# Securing DNS Service
# ------------------------------------------------------------------------

# Disable DNS Service
# -------------------
serveradmin stop dns

# ------------------------------------------------------------------------
# Securing Firewall Service
# ------------------------------------------------------------------------

# Start Firewall service
# ----------------------
serveradmin start ipfilter

# Enable stealth mode
# -------------------
serveradmin settings ipfilter:blackHoleTCP = true
serveradmin settings ipfilter:blackHoleUDP = true

# View the Firewall service log
# -----------------------------
tail /var/log/ipfw.log

# ------------------------------------------------------------------------
# Securing NAT Service
# ------------------------------------------------------------------------

# Disable NAT service
# -------------------
serveradmin stop nat

# ------------------------------------------------------------------------
# Securing iCal Service
# ------------------------------------------------------------------------

# disable iCal service
# --------------------------------
serveradmin stop calendar
```

```
# Choose an authentication method for iCal service
# To enable all auth methods:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar

# To choose Digest auth only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "no"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar

# For Kerberos only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "no"
serveradmin stop calendar; sudo serveradmin start calendar

# Enable secure network traffic using SSL transport
serveradmin settings calendar:SSLPort = 8443

# View the iCal service log
tail /var/log/caldavd/access.log

# Disable iChat service
serveradmin stop jabber

# Securely configure iChat service
# To select an iChat server certificate:
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"

# (Or replace the path with the full path to the certificate that you want
# to select.)
# Restart the service if it is running
serveradmin stop jabber; sudo serveradmin start jabber

# To select an iChat server auth method you would use one of the following:
serveradmin settings jabber:authLevel = "ANYMETHOD"
serveradmin settings jabber:authLevel = "KERBEROS"
serveradmin settings jabber:authLevel = "STANDARD"

# Then restart the service:
serveradmin stop jabber
serveradmin start jabber

# Select a certificate
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"

# View the iChat service log
tail /var/log/server.log | grep jabberd
```

```
# ------------------------------------------------------------------
# Securing Wiki Service
# ------------------------------------------------------------------

# Disable Web service
serveradmin stop teams

# View the Wiki service log
tail /Library/Logs/wikid/access.log

# Disable Podcast Producer service
serveradmin stop pcast

# View the Podcast Producer service log
tail /Library/Logs/pcastserverd/pcastserverd_out.log

# ------------------------------------------------------------------
# Securing Mail Service
# ------------------------------------------------------------------

# Disable Mail service protocols
serveradmin settings mail:imap:enable_pop = no
serveradmin settings mail:imap:enable_imap = no
serveradmin settings mail:postfix:enable_smtp = no

# Set the POP authentication method
serveradmin settings mail:imap:pop_auth_apop = no
serveradmin settings mail:imap:pop_auth_clear = no
serveradmin settings mail:imap:pop_auth_gssapi = no

# Set SSL transport for POP connections
serveradmin settings mail:imap:tls_server_options = "use"

# Set secure IMAP authentication
serveradmin settings mail:imap:imap_auth_login = no
serveradmin settings mail:imap:imap_auth_plain = no
serveradmin settings mail:imap:imap_auth_gssapi = no
serveradmin settings mail:imap:imap_auth_clear = no
serveradmin settings mail:imap:imap_auth_cram_md5 = no

# Configure SSL transport for IMAP connections (same as POP)
serveradmin settings mail:imap:tls_server_options = "use"

# Allow secure SMTP authentication
serveradmin settings mail:postfix:smtpd_sasl_auth_enable = yes
serveradmin settings mail:postfix:smtpd_use_pw_server = "yes"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:0 = "gssapi"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:1 =
     "cram-md5"
```

```
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:2 = "login"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:3 = "plain"

# Configure SSL transport for SMTP connections
serveradmin settings mail:postfix:smtpd_use_tls = "yes"

# Enable a user's mail access using ACLs
dseditgroup -o edit -a $USER -t user com.apple.access_mail

# Restrict SMTP relay
serveradmin settings mail:postfix:mynetworks_enabled = yes

# Reject unauthorized SMTP connections
serveradmin settings mail:postfix:smtp_reject_list_enabled = yes
serveradmin settings mail:postfix:smtp_reject_list:_array_index:0 =
     "$NETWORK"

# Reject mail from blacklisted senders
serveradmin settings mail:postfix:black_hole_domains:_array_index:0 =
     "$BLACKLIST_SERVER"
serveradmin settings mail:postfix:maps_rbl_domains_enabled = yes

# Enable junk mail screening
serveradmin settings mail:postfix:spam_scan_enabled = yes

# Train the filter
sa-learn --showdots --spam $JUNK_DIRECTORY/*
sa-learn --showdots --ham $NON_JUNK_DIRECTORY/*

# Automatically train the junk mail filter
/etc/mail/spamassassin/learn_junk_mail

# Allow mail by language and locale
serveradmin settings mail:postfix:spam_ok_languages = "en fr de"
serveradmin settings mail:postfix:spam_ok_locales = "en"

# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes

# View a Mail service log
tail /var/log/mail.log

# ------------------------------------------------------------------------
# Securing Antivirus Services
# ------------------------------------------------------------------------

# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes
```

```
# View a virus log
tail /var/log/amavisd.log

# ------------------------------------------------------------------
# Securing File Services
# ------------------------------------------------------------------

# Disable file sharing services
serveradmin stop afp
serveradmin stop smb
serveradmin stop ftp
serveradmin stop nfs

# Securely configure AFP Service
serveradmin settings afp:registerNSL = no
serveradmin settings afp:attemptAdminAuth = no
serveradmin settings afp:clientSleepOnOff = no
serveradmin settings afp:idleDisconnectOnOff = yes
serveradmin settings afp:authenticationMode = "kerberos"
serveradmin settings afp:activityLog = yes
serveradmin settings afp:guestAccess = no

# Configure FTP to provide anonymous FTP downloads
serveradmin settings ftp:logSecurity:anonymous = yes
serveradmin settings ftp:logSecurity:guest = yes
serveradmin settings ftp:logSecurity:real = yes
serveradmin settings ftp:maxRealUsers = 1
serveradmin settings ftp:enableMacBinAndDmgAutoConversion = no
serveradmin settings ftp:authLevel = "KERBEROS"
serveradmin settings ftp:anonymousAccessPermitted = yes
serveradmin settings ftp:bannerMessage = "$BANNER"
serveradmin settings ftp:maxAnonymousUsers = 500
serveradmin settings ftp:administratorEmailAddress = "user@domain.com"
serveradmin settings ftp:logCommands:anonymous = yes
serveradmin settings ftp:logCommands:guest = yes
serveradmin settings ftp:logCommands:real = yes
serveradmin settings ftp:loginFailuresPermitted = 1
serveradmin settings ftp:welcomeMessage = "$WELCOME"

# Securely configure Windows file sharing service
serveradmin settings smb:wins support = no
serveradmin settings smb:domain master = no
serveradmin settings smb:map to guest = "Never"
serveradmin settings smb:auth methods = "odsam"
serveradmin settings smb:ntlm auth = "no"
serveradmin settings smb:max smbd processes = 1000
serveradmin settings smb:log level = 1
serveradmin settings smb:preferred master = no
serveradmin settings smb:os level = 65
```

```
# ------------------------------------------------------------------
# Securing Web Service
# ------------------------------------------------------------------

# Disable Web service
serveradmin stop web

# Disable web options
serveradmin settings web:Modules:_array_id:authz_host_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_fs_module:enabled = no
serveradmin settings web:Modules:_array_id:apple_spotlight_module:enabled =
     no
serveradmin settings web:Sites:_array_id:$SITE:SpotlightIndexing = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:AllowOverride = "None"
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:IfModule:_array_id:mod_dav.c:DAV = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:Includes = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:ExecCGI = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:Indexes = no
serveradmin settings web:Sites:_array_id:default_default:SpotlightIndexing =
     no

# configure Apache to prompt you for a passphrase when it starts
serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL
     PassPhraseDialog=builtin

# View logs
tail /var/log/apache2/access_log

# Disable Blog service
serveradmin settings web:Sites:_array_id:$SITE:weblog = no

# ------------------------------------------------------------------
# Securing Tomcat
# ------------------------------------------------------------------

# Stop Tomcat using Server Admin
/Library/Tomcat/bin/startup.sh stop

# ------------------------------------------------------------------
# Securing MySQL
# ------------------------------------------------------------------

# Turn MySQL service on
serveradmin stop mysql
```

```
# Configure MySQL service settings
serveradmin settings mysql:allowNetwork = yes

# View MySQL service logs
tail /Library/Logs/MySQL.log

# ------------------------------------------------------------------
# Securing WebObjects
# ------------------------------------------------------------------

# Disable the WebObjects service
serveradmin stop webobjects

# Securing Client Configuration Management Services
# ================================================
# If the intended target is a client system, the target for the dscl
# commands should be "/LDAPv3/127.0.0.1". If the management target is the
# server itself, then the target should be ".".

# Disable Front Row
dscl /LDAPv3/127.0.0.1 mcxset  /Computers/$COMPUTER com.apple.frontrow
     PreventActivation always -bool 1

# Setting up a list of accessible applications
# --------------------------------------------
# Allow access to applications stored on the user's local hard disk
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess OpenItemsInternalDrive always -bool 1

# Allow helper applications
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess ApprovedAppLaunchesOthers always -bool 1

# Allow UNIX tools
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess AllowUnbundledApps always -bool 1

# Managing Dock Preferences
# -------------------------
# Set Dock hiding
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide always -bool 1

# Managing Finder Preferences
# ---------------------------
# Manage Finder preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     AppleShowAllExtensions-immutable always -bool 1
```

```
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitBurn always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitConnectTo always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitEject always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToFolder always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToiDisk always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowHardDrivesOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowMountedServersOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowRemovableMediaOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     AppleShowAllExtensions always -bool 1

# Managing Login Preferences
# --------------------------
# Manage Login preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     LoginwindowText always -string "$LOGIN WINDOW MESSAGE"
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     mcx_UseLoginWindowText always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     RestartDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     ShutDownDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     SHOWFULLNAME always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     DisableConsoleAccess always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     MultipleSessionEnabled always -bool 0

# Managing Network Preferences
# ----------------------------
# Manage Network preferences
networksetup -setwebproxystate Ethernet on
networksetup -setwebproxy Ethernet "http://$SERVER" 8008

networksetup -setpassiveftp Ethernet on

# Managing Parental Control Preferences
# -------------------------------------
# Hide profanity
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.Dictionary
     parentalControl always -bool 1
```

```
# Managing Printing Preferences
# ----------------------------
# Manage Printing preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     RequireAdminToAddPrinters always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     AllowLocalPrinters always -bool 0

# Managing Software Update Preferences
# -----------------------------------
# Manage Software Update preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.SoftwareUpdate
     CatalogURL always -string "http:/$SERVER:8088/index.sucatalog"

# Managing Universal Access Preferences
# -------------------------------------
# Manage Universal Access preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKey always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyBeepOnModifier always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyShowWindow always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewDriver always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewShowPreview always -bool 0

# ------------------------------------------------------------------------
# Securing NetBoot Service
# ------------------------------------------------------------------------

# Disable NetBoot
serveradmin stop netboot

# Securely configure NetBoot
defaults rename /etc/bootpd allow_disabled allow

# View NetBoot service logs
tail /var/log/system.log | grep bootpd

# ------------------------------------------------------------------------
# Securing Software Update Service
# ------------------------------------------------------------------------

# Disable Software Update
serveradmin stop swupdate

# Specify which client can access software updates
serveradmin settings swupdate:autoEnable = no
```

```
# View Software Update service logs
tail /var/log/swupd/swupd_*

# ------------------------------------------------------------------
# Securing Directory Services
# ------------------------------------------------------------------

# Configure the Open Directory role
slapconfig -createldapmasterandadmin $ADMIN $ADMIN_FULL_NAME $ADMIN_UID
     $SEARCH_BASE $REALM

# Start Kerberos manually on an Open Directory master
kdcsetup -a $ADMIN $REALM

# Change the global password policy of user accounts in the same domain
pwpolicy -a $ADMIN_USER -setglobalpolicy "minChars=4
     maxFailedLoginAttempts=3"

# Set the binding policy for an Open Directory master
slapconfig -setmacosxodpolicy -binding required

# Set the security policy for an Open Directory master
slapconfig -setmacosxodpolicy -cleartext blocked

# ------------------------------------------------------------------
# Securing RADIUS Service
# ------------------------------------------------------------------

# Disable RADIUS service
radiusconfig stop

# Use a custom certificate
serveradmin settings radius:eap.conf:CA_file = "/etc/certificates/$CA_CRT"
serveradmin settings radius:eap.conf:private_key_file =
     "/etc/certificates/$KEY"
serveradmin settings radius:eap.conf:private_key_password = "$PASS"
serveradmin settings radius:eap.conf:certificate_file =
     "/etc/certificates/$CERT"

# Edit RADIUS access
dseditgroup -o edit -a $USER -t user com.apple.access_radius

# View the Radius service log
tail /var/log/radius/radius.log

# ------------------------------------------------------------------
# Securing Print Service
# ------------------------------------------------------------------

# Disable Print service
serveradmin stop print
```

```
# Set administrator SACL permissions for Print service
dseditgroup -o edit -a $USER -t user com.apple.monitor_print

# Configure Kerberos for Print service
cp /etc/cups/cupsd.conf $TEMP_FILE
/usr/bin/sed "/^DefaultAuthType.*/s//DefaultAuthType Negotiate/g" $TEMP_FILE
     > /etc/cups/cupsd.conf

# View Print service logs
tail /Library/Logs/PrintService/PrintService_admin.log

# ------------------------------------------------------------------------
# Securing Multimedia Services
# ------------------------------------------------------------------------

# Disable QTSS
serveradmin stop qtss

# Configure a streaming server
serveradmin settings
     qtss:server:bind_ip_addr:_array_index:0 = "$Bind_IP_Address"

# Serve QuickTime streams over HTTP port 80
$ serveradmin settings
     qtss:server:rtsp_port:_array_index:0 = 554
     qtss:server:rtsp_port:_array_index:1 = 80
     qtss:server:rtsp_port:_array_index:2 = 8000
     qtss:server:rtsp_port:_array_index:3 = 8001

# Change the MP3 broadcast password
serveradmin settings
qtss:modules:_array_id:QTSSMP3StreamingModule:mp3_broadcast_password =
     "password"

# Create a broadcast user name and password on the streaming server
serveradmin settings
     qtss:modules:_array_id:QTSSReflectorModule:allow_broadcasts = yes

# Add a user account
qtpasswd $USER

# Adding groups
echo "$GROUP_NAME: $USER1 $USER2 $USER3" /Library/QuickTimeStreaming/Config/
     qtgroups

# Change a user password
qtpasswd $USER

# View the QTSS log
tail /Library/QuickTimeStreaming/Logs/$LOG_FILE
```

```
# ------------------------------------------------------------------
# Xgrid Service
# ------------------------------------------------------------------

# Disable Xgrid service
serveradmin stop xgrid

# Configure an Xgrid agent on the server
/usr/sbin/xgridctl agent stop

# Configure an Xgrid controller
serveradmin settings xgrid:ControllerSettings:Enabled = yes
serveradmin settings xgrid:ControllerSettings:prefs:ClientAuthentication =
     Password
serveradmin settings xgrid:ControllerSettings:ClientPassword =
     $Xgrid_Client_Password

# ------------------------------------------------------------------
# Maintaining System Integrity
# ------------------------------------------------------------------

# Validate application bundle integrity.
codesign -v $code_path

# Verify a requirement.
codesign -v -R="identifier com.apple.Mail and anchor apple" /Applications/
     Mail.app

# Install the common criteria tools software
installer -pkg CommonCriteriaTools.pkg -target /

# Enable auditing
cp /etc/hostconfig /tmp/test

if /usr/bin/grep AUDIT /etc/hostconfig
then
  /usr/bin/sed "/^AUDIT.*/s//AUDIT=-YES-/g" /tmp/test > /etc/hostconfig
else
  /bin/echo AUDIT=-YES- >> /etc/hostconfig
fi

# View logs in Server Admin
# Use tail or more to view the log files.
# The audit files are individually named based on the date.

/usr/bin/tail $AUDIT_FILE

# ------------------------------------------------------------------
# Protecting System Hardware
# ------------------------------------------------------------------
# Securing Wi-Fi Hardware
```

```
# ----------------------
# Remove AppleAirport kernel extensions
srm -r /System/Library/Extensions/AppleAirPort.kext
srm -r /System/Library/Extensions/AppleAirPort2.kext
srm -r /System/Library/Extensions/AppleAirPortFW.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Removing BlueTooth Software
# ---------------------------
# Remove Bluetooth kernel extensions
srm -r /System/Library/Extensions/IOBluetoothFamily.kext
srm -r /System/Library/Extensions/IOBluetoothHIDDriver.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Removing Audio Recording Software
# ---------------------------------
# Remove Audio Recording kernel extensions
srm -r /System/Library/Extensions/AppleOnboardAudio.kext
srm -r /System/Library/Extensions/AppleUSBAudio.kext
srm -r /System/Library/Extensions/AppleDeviceTreeUpdater.kext
srm -r /System/Library/Extensions/IOAudioFamily.kext
srm -r /System/Library/Extensions/VirtualAudioDriver.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Removing Video Recording Software
# ---------------------------------
# Remove Video Recording kernel extensions.

# Remove external iSight camera.
srm -rf /System/Library/Extensions/Apple_iSight.kext

# Remove internal iSight camera.
srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/
     AppleUSBVideoSupport.kext

# Remove Extensions cache files.
touch /System/Library/Extensions

# Removing USB Support
# --------------------
# Remove USB kernel extensions
srm -r /System/Library/Extensions/IOUSBMassStorageClass.kext

# Remove Extensions cache files
touch /System/Library/Extensions
```

```
# Securing FireWire Hardware
# ----------------------------
# Remove FireWire kernel extensions
srm -r /System/Library/Extensions/IOFireWireSerialBusProtocolTransport.kext

# Remove Extensions cache files
touch /System/Library/Extensions

# Securing Global System Settings
# ------------------------------------------------------------------------
# Configuring Open Firmware Settings
# ----------------------------------
# Secure startup by setting security-mode. Replace $mode-value with
# “command” or “full”.
nvram security-mode=”$mode-value”

# Verify security-mode setting.
nvram -p

# Enabling Access Warning for the Login Window
# --------------------------------------------
# Create a login window access warning.
defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText
     “Warning Text”
# You can also use the BannerSample project to create an access warning.

# ---------------------------------------------------------------------
# Securing System Preferences
# ---------------------------------------------------------------------
# Securing MobileMe Preferences
# -------------------------
# Disable Sync options
/System/Library/CoreServices/dotmacsynclient --removeclient
     com.apple.DotMacSync

# Disable iDisk Syncing
defaults -currentHost delete com.apple.idisk

# Securing Accounts Preferences
# -----------------------------
# Change an account’s password on a client system.
# Don’t use this commands if other users are also logged in
sudo dscl /LDAPv3/127.0.0.1 passwd /Users/$User_name $Oldpass $Newpass

# Change an account’s password on a server.
# Don’t use this commands if other users are also logged in
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass

# Make sure there is no password hint set.
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint -
     int 0
```

```
# Set the login options to display name and password in the login window.
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool
     yes

# Disable Show the Restart, Sleep, and ShutDown Buttons.
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
     bool yes

# Disable fast user switching. This command does not prevent multiple users
# from being logged in.
defaults write /Library/Preferences/.GlobalPreferences
     MultipleSessionEnabled -bool NO

# Securing Appearance Preferences
# ------------------------------
# Disable display of recent applications.
defaults write com.apple.recentitems Applications -dict MaxAmount 0

# Securing Bluetooth Preferences
# ------------------------------
# Turn Bluetooth off
defaults write /Library/Preferences/com.apple.Bluetooth ControllerPowerState
     -int 0


# Securing CDs & DVDs Preferences
# ------------------------------
# Disable blank CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.cd.appeared -dict action 1

# Disable music CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.music.appeared -dict action 1

# Disable picture CD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.cd.picture.appeared -dict action 1

# Disable blank DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.blank.dvd.appeared -dict action 1

# Disable video DVD automatic action
defaults write /Library/Preferences/com.apple.digihub
     com.apple.digihub.dvd.video.appeared -dict action 1

# Securing Date & Time Preferences
# ------------------------------
# Set the NTP server.
cat >> /etc/ntp.conf << END server time.apple.com END
```

```
# Set the Date and Time.
systemsetup -settimezone $Time_Zone

# Disable NTPD if there is no trusted NTPD available.
launchctl unload -w org.ntp.ntpd.plist

# Securing Desktop & Screen Saver Preferences
# -----------------------------------------
# Set idle time for screen saver. XX is the idle time in seconds.
defaults -currentHost write com.apple.screensaver idleTime -int XX

# Set host corner to activate screen saver.
# wvous-bl-corner (bottom-left)
# wvous-br-corner(bottom-right)
# wvous-tl-corner (top-left)
# wvous-tr-corner (top-right)
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-corner
     -int 5

# Set modifier key to 0 wvous-corner_code-modifier
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
     modifier -int 0


# Securing Dock Preferences
# -------------------------
# Automatically hide and show Dock
defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Restart dock
killall -HUP Dock

# Securing Energy Saver Preferences
# ---------------------------------
# Disable computer sleep.
pmset -a sleep 0

# Enable hard drive sleep.
pmset -a disksleep $minutes

# Disable Wake for Ethernet network administrator access.
pmset -a womp 0

# Disable Restart automatically after power failure.
pmset -a autorestart 0

# Securing Expose & Spaces Preferences
# ------------------------------------
# Disable dashboard.
defaults write com.apple.dashboard mcx-disabled -boolean YES
```

```
# Securing Keyboard & Mouse Preferences
# -------------------------------------
# Disable Bluetooth Devices to wake computer
defaults write /Library/Preferences/com.apple.Bluetooth.plist
     BluetoothSystemWakeEnable -bool 0

# Securing Network Preferences
# ----------------------------
# Disable IPv6
# The interface value can be AirPort, Bluetooth, Ethernet, or FireWire.
networksetup -setv6off $interface

# Securing Printer & Fax Preferences
# ----------------------------------
# Disable the receiving of faxes.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist

# Disable printer sharing.
cp /etc/cups/cupsd.conf $TEMP_FILE
if /usr/bin/grep "Port 631" /etc/cups/cupsd.conf
then
     /usr/bin/sed "/^Port 631.*/s//Listen localhost:631/g" $TEMP_FILE
     /etc/cups/cupsd.conf
else
     echo "Printer Sharing not on"
fi

# Securing Security Preferences
# -----------------------------
# Enable Require password to wake this computer from sleep or screen
# saver.
defaults -currentHost write com.apple.screensaver askForPassword -int 1

# Disable automatic login.
defaults write /Library/Preferences/.GlobalPreferences
     com.apple.userspref.DisableAutoLogin -bool yes
# Disabling automatic login leaves the /etc/kcpasswd file behind.
# This file contains an obfuscated copy of the user password.
# Erase the /etc/kcpasswd file.
srm /etc/kcpasswd

# Require password to unlock each System Preference pane.
# Edit the /etc/authorization file using a text editor.
# Find <key>system.preferences<key>.
# Then find <key>shared<key>.
# Then replace <true/> with <false/>.
# Disable automatic logout.
defaults write /Library/Preferences/.GlobalPreferences
     com.apple.autologout.AutoLogOutDelay -int 0
```

```
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory UseEncryptedSwap
     -bool yes

# Disable IR remote control.
defaults write /Library/Preferences/com.apple.driver.AppleIRController
     DeviceEnabled -bool no

# Enable FileVault.
# To enable FileVault for new users, use this command.
/System/Library/CoreServices/ManagedClient.app/Contents/Resources/
     createmobileaccount

# Enable firewall, where value is:
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
defaults write /Library/Preferences/com.apple.alf globalstate -int value

# Enable Stealth mode.
defaults write /Library/Preferences/com.apple.alf stealthenabled 1

# Enable firewall logging.
defaults write /Library/Preferences/com.apple.alf loggingenabled 1

# Securing Sharing Preferences
# ----------------------------
# Change the computer name, where $host_name is the name of the computer.
# This command does not change the Bonjour host name.
systemsetup -setcomputername $host_name

# Change the Bonjour host name, where $Bon_host_name must not contain
# spaces or other non-DNS characters.
scutil --set LocalHostName $Bon_host_name

# Securing Software Updates Preferences
# -------------------------------------
# Disable check for updates and Download important updates automatically
softwareupdate --schedule off

# Securing Sound Preferences
# --------------------------
# Disable internal microphone or line-in.
# This command does not change the input volume for all input devices. It
# only sets the default input device volume to zero.
osascript -e “set volume input volume 0”
```

```
# Securing Speech Preferences
# ----------------------------
# Disable Speech Recognition
defaults write "com.apple.speech.recognition.AppleSpeechRecognition.prefs"
     StartSpeakableItems -bool false

# Disable Text to Speech settings
defaults write "com.apple.speech.synthesis.general.prefs"
     TalkingAlertsSpeakTextFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenNotificationAppActivationFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
     SpokenUIUseSpeakingHotKeyFlag -bool false
defaults delete "com.apple.speech.synthesis.general.prefs"
     TimeAnnouncementPrefs


# Securing Spotlight Preferences
# ----------------------------
# Disable Spotlight for a volume and erase its current meta data. Where
# $volumename is the name of the volume.
$ mdutil -E -i off $volumename

# Securing Startup Disk Preferences
# ----------------------------
# Set startup disk
systemsetup -setstartupdisk $path

# Securing Time Machine Preferences
# --------------------------------
# Enable Time Machine
defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1

# ---------------------------------------------------------------------
# Using Disk Utility to Securely Erase Free Space
# ---------------------------------------------------------------------
# Overwrite a device with zeroes.
diskutil zeroDisk /dev/device

# Secure erase (7-pass) free space on a volume.
diskutil secureErase freespace 2 /dev/device

# Secure erase (7-pass) a volume.
diskutil secureErase 2 /dev/device

# Securing System Swap and Hibernation Storage
# ------------------------------------------
# Enable secure virtual memory
defaults write /Library/Preferences/com.apple.virtualMemory UseEncryptedSwap
     -bool YES
```

```
# ------------------------------------------------------------------
# Setting General Protocols
# ------------------------------------------------------------------

# Disable NTP
# -----------
systemsetup -setusingnetworktime off

# Disable SNMP
# ------------
service org.net-snmp.snmpd stop

# Enable SSH
# ----------
service ssh start


# Set SACL permissions for a service
# ----------------------------------
dseditgroup -o edit -a $USER -t user $SACL_GROUP

# ------------------------------------------------------------------
# Enabling IPv6
# ------------------------------------------------------------------

# Enable IPv6
# -------------------------------
networksetup -setv6on [networkservice]

# ------------------------------------------------------------------
# Securing DHCP Service
# ------------------------------------------------------------------

# Disable DHCP Service
# --------------------
serveradmin stop dhcp

# Configuring DHCP Services
# -------------------------
# Set a DHCP subnet's DNS, LDAP, and WINS parameters to no value
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:dhcp_domain_name_server:_array_index:0 = ""
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:dhcp_ldap_url:_array_index:0 = -empty_array
serveradmin set dhcp:configuation:subnets:_array_id:9ADA7CCF-D9AC-4381-AEE5-
     BED51A44775D:WINS_node_type =" NOT SET"
```

```
# ------------------------------------------------------------------
# Securing DNS Service
# ------------------------------------------------------------------

# Disable DNS Service
# -------------------
serveradmin stop dns

# ------------------------------------------------------------------
# Securing Firewall Service
# ------------------------------------------------------------------

# Start Firewall service
# ----------------------
serveradmin start ipfilter

# Enable stealth mode
# -------------------
serveradmin settings ipfilter:blackHoleTCP = true
serveradmin settings ipfilter:blackHoleUDP = true

# View the Firewall service log
# -----------------------------
tail /var/log/ipfw.log

# ------------------------------------------------------------------
# Securing NAT Service
# ------------------------------------------------------------------

# Disable NAT service
# -------------------
serveradmin stop nat

# ------------------------------------------------------------------
# Securing iCal Service
# ------------------------------------------------------------------

# disable iCal service
# --------------------------------
serveradmin stop calendar

# Choose an authentication method for iCal service
# To enable all auth methods:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar

# To choose Digest auth only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "no"
serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
serveradmin stop calendar; sudo serveradmin start calendar
```

```
# For Kerberos only:
serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
serveradmin settings calendar:Authentication:Digest:Enabled = "no"
serveradmin stop calendar; sudo serveradmin start calendar

# Enable secure network traffic using SSL transport
serveradmin settings calendar:SSLPort = 8443

# View the iCal service log
tail /var/log/caldavd/access.log

# Disable iChat service
serveradmin stop jabber

# Securely configure iChat service
# To select an iChat server certificate:
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"

# (Or replace the path with the full path to the certificate that you want
# to select.)
# Restart the service if it is running
serveradmin stop jabber; sudo serveradmin start jabber

# To select an iChat server auth method you would use one of the following:
serveradmin settings jabber:authLevel = "ANYMETHOD"
serveradmin settings jabber:authLevel = "KERBEROS"
serveradmin settings jabber:authLevel = "STANDARD"

# Then restart the service:
serveradmin stop jabber
serveradmin start jabber

# Select a certificate
serveradmin settings jabber:sslKeyFile = "/etc/certificates/Default.crtkey"

# View the iChat service log
tail /var/log/server.log | grep jabberd

# ------------------------------------------------------------------------
# Securing Wiki Service
# ------------------------------------------------------------------------

# Disable Web service
serveradmin stop teams

# View the Wiki service log
tail /Library/Logs/wikid/access.log

# Disable Podcast Producer service
sudo serveradmin stop pcast
```

```
# View the Podcast Producer service log
tail /Library/Logs/pcastserverd/pcastserverd_out.log

# ------------------------------------------------------------------
# Securing Mail Service
# ------------------------------------------------------------------

# Disable Mail service protocols
serveradmin settings mail:imap:enable_pop = no
serveradmin settings mail:imap:enable_imap = no
serveradmin settings mail:postfix:enable_smtp = no

# Set the POP authentication method
serveradmin settings mail:imap:pop_auth_apop = no
serveradmin settings mail:imap:pop_auth_clear = no
serveradmin settings mail:imap:pop_auth_gssapi = no


# Set SSL transport for POP connections
serveradmin settings mail:imap:tls_server_options = "use"

# Set secure IMAP authentication
serveradmin settings mail:imap:imap_auth_login = no
serveradmin settings mail:imap:imap_auth_plain = no
serveradmin settings mail:imap:imap_auth_gssapi = no
serveradmin settings mail:imap:imap_auth_clear = no
serveradmin settings mail:imap:imap_auth_cram_md5 = no

# Configure SSL transport for IMAP connections (same as POP)
serveradmin settings mail:imap:tls_server_options = "use"

# Allow secure SMTP authentication
serveradmin settings mail:postfix:smtpd_sasl_auth_enable = yes
serveradmin settings mail:postfix:smtpd_use_pw_server = "yes"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:0 = "gssapi"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:1 =
     "cram-md5"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:2 = "login"
serveradmin settings
     mail:postfix:smtpd_pw_server_security_options:_array_index:3 = "plain"

# Configure SSL transport for SMTP connections
serveradmin settings mail:postfix:smtpd_use_tls = "yes"

# Enable a user's mail access using ACLs
dseditgroup -o edit -a $USER -t user com.apple.access_mail
```

```
# Restrict SMTP relay
serveradmin settings mail:postfix:mynetworks_enabled = yes

# Reject unauthorized SMTP connections
serveradmin settings mail:postfix:smtp_reject_list_enabled = yes
serveradmin settings mail:postfix:smtp_reject_list:_array_index:0 =
     "$NETWORK"

# Reject mail from blacklisted senders
serveradmin settings mail:postfix:black_hole_domains:_array_index:0 =
     "$BLACKLIST_SERVER"
serveradmin settings mail:postfix:maps_rbl_domains_enabled = yes

# Enable junk mail screening
serveradmin settings mail:postfix:spam_scan_enabled = yes

# Train the filter
sa-learn --showdots --spam $JUNK_DIRECTORY/*
sa-learn --showdots --ham $NON_JUNK_DIRECTORY/*
# Automatically train the junk mail filter
/etc/mail/spamassassin/learn_junk_mail

# Allow mail by language and locale
serveradmin settings mail:postfix:spam_ok_languages = "en fr de"
serveradmin settings mail:postfix:spam_ok_locales = "en"

# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes

# View a Mail service log
tail /var/log/mail.log

# ------------------------------------------------------------------------
# Securing Antivirus Services
# ------------------------------------------------------------------------

# Enable virus screening
serveradmin settings mail:postfix:virus_scan_enabled = yes

# View a virus log
tail /var/log/amavisd.log

# ------------------------------------------------------------------------
# Securing File Services
# ------------------------------------------------------------------------

# Disable file sharing services
serveradmin stop afp
serveradmin stop smb
serveradmin stop ftp
serveradmin stop nfs
```

```
# Securely configure AFP Service
serveradmin settings afp:registerNSL = no
serveradmin settings afp:attemptAdminAuth = no
serveradmin settings afp:clientSleepOnOff = no
serveradmin settings afp:idleDisconnectOnOff = yes
serveradmin settings afp:authenticationMode = "kerberos"
serveradmin settings afp:activityLog = yes
serveradmin settings afp:guestAccess = no

# Configure FTP to provide anonymous FTP downloads
serveradmin settings ftp:logSecurity:anonymous = yes
serveradmin settings ftp:logSecurity:guest = yes
serveradmin settings ftp:logSecurity:real = yes
serveradmin settings ftp:maxRealUsers = 1
serveradmin settings ftp:enableMacBinAndDmgAutoConversion = no
serveradmin settings ftp:authLevel = "KERBEROS"
serveradmin settings ftp:anonymousAccessPermitted = yes
serveradmin settings ftp:bannerMessage = "$BANNER"
serveradmin settings ftp:maxAnonymousUsers = 500
serveradmin settings ftp:administratorEmailAddress = "user@domain.com"
serveradmin settings ftp:logCommands:anonymous = yes
serveradmin settings ftp:logCommands:guest = yes
serveradmin settings ftp:logCommands:real = yes
serveradmin settings ftp:loginFailuresPermitted = 1
serveradmin settings ftp:welcomeMessage = "$WELCOME"

# Securely configure Windows file sharing service
serveradmin settings smb:wins support = no
serveradmin settings smb:domain master = no
serveradmin settings smb:map to guest = "Never"
serveradmin settings smb:auth methods = "odsam"
serveradmin settings smb:ntlm auth = "no"
serveradmin settings smb:max smbd processes = 1000
serveradmin settings smb:log level = 1
serveradmin settings smb:preferred master = no
serveradmin settings smb:os level = 65

# ------------------------------------------------------------------
# Securing Web Service
# ------------------------------------------------------------------

# Disable Web service
serveradmin stop web

# Disable web options
serveradmin settings web:Modules:_array_id:authz_host_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_module:enabled = no
serveradmin settings web:Modules:_array_id:dav_fs_module:enabled = no
serveradmin settings web:Modules:_array_id:apple_spotlight_module:enabled =
     no
serveradmin settings web:Sites:_array_id:$SITE:SpotlightIndexing = no
```

```
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:AllowOverride = "None"
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:IfModule:_array_id:mod_dav.c:DAV = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:Includes = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:ExecCGI = no
serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/Library/
     WebServer/Documents:Options:Indexes = no
serveradmin settings web:Sites:_array_id:default_default:SpotlightIndexing =
     no

# configure Apache to prompt you for a passphrase when it starts
serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL
     PassPhraseDialog=builtin


# View logs
tail /var/log/apache2/access_log

# Disable Blog service
serveradmin settings web:Sites:_array_id:$SITE:weblog = no

# ------------------------------------------------------------------------
# Securing Tomcat
# ------------------------------------------------------------------------

# Stop Tomcat using Server Admin
/Library/Tomcat/bin/startup.sh stop

# ------------------------------------------------------------------------
# Securing MySQL
# ------------------------------------------------------------------------

# Turn MySQL service on
serveradmin stop mysql

# Configure MySQL service settings
serveradmin settings mysql:allowNetwork = yes

# View MySQL service logs
tail /Library/Logs/MySQL.log

# ------------------------------------------------------------------------
# Securing WebObjects
# ------------------------------------------------------------------------

# Disable the WebObjects service
serveradmin stop webobjects
```

```
# Securing Client Configuration Management Services
# ================================================
# If the intended target is a client system, the target for the dscl
# commands should be "/LDAPv3/127.0.0.1". If the management target is the
# server itself, then the target should be ".".

# Disable Front Row
dscl /LDAPv3/127.0.0.1 mcxset  /Computers/$COMPUTER com.apple.frontrow
     PreventActivation always -bool 1

# Setting up a list of accessible applications
# --------------------------------------------
# Allow access to applications stored on the user's local hard disk
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess OpenItemsInternalDrive always -bool 1



# Allow helper applications
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess ApprovedAppLaunchesOthers always -bool 1

# Allow UNIX tools
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
     com.apple.applicationaccess AllowUnbundledApps always -bool 1

# Managing Dock Preferences
# -------------------------
# Set Dock hiding
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock
     autohide always -bool 1

# Managing Finder Preferences
# ---------------------------
# Manage Finder preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     AppleShowAllExtensions-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitBurn always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitConnectTo always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitEject always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToFolder always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ProhibitGoToiDisk always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowHardDrivesOnDesktop-immutable always -bool 1
```

```
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowMountedServersOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
     ShowRemovableMediaOnDesktop-immutable always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     AppleShowAllExtensions always -bool 1

# Managing Login Preferences
# --------------------------
# Manage Login preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     LoginwindowText always -string "$LOGIN WINDOW MESSAGE"
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     mcx_UseLoginWindowText always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     RestartDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     ShutDownDisabled always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     SHOWFULLNAME always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.loginwindow
     DisableConsoleAccess always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
     MultipleSessionEnabled always -bool 0

# Managing Network Preferences
# ----------------------------
# Manage Network preferences
networksetup -setwebproxystate Ethernet on
networksetup -setwebproxy Ethernet "http://$SERVER" 8008

networksetup -setpassiveftp Ethernet on

# Managing Parental Control Preferences
# -------------------------------------
# Hide profanity
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.Dictionary
     parentalControl always -bool 1

# Managing Printing Preferences
# -----------------------------
# Manage Printing preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     RequireAdminToAddPrinters always -bool 1
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
     AllowLocalPrinters always -bool 0
```

```
# Managing Software Update Preferences
# -----------------------------------
# Manage Software Update preferences
dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.SoftwareUpdate
     CatalogURL always -string "http:/$SERVER:8088/index.sucatalog"

# Managing Universal Access Preferences
# -----------------------------------
# Manage Universal Access preferences
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKey always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyBeepOnModifier always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     stickyKeyShowWindow always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewDriver always -bool 0
dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2 com.apple.universalaccess
     closeViewShowPreview always -bool 0

# ------------------------------------------------------------------------
# Securing NetBoot Service
# ------------------------------------------------------------------------

# Disable NetBoot
serveradmin stop netboot

# Securely configure NetBoot
defaults rename /etc/bootpd allow_disabled allow

# View NetBoot service logs
tail /var/log/system.log | grep bootpd

# ------------------------------------------------------------------------
# Securing Software Update Service
# ------------------------------------------------------------------------

# Disable Software Update
serveradmin stop swupdate

# Specify which client can access software updates
serveradmin settings swupdate:autoEnable = no

# View Software Update service logs
tail /var/log/swupd/swupd_*
```

```
# ------------------------------------------------------------------
# Securing Directory Services
# ------------------------------------------------------------------

# Configure the Open Directory role
slapconfig -createldapmasterandadmin $ADMIN $ADMIN_FULL_NAME $ADMIN_UID
     $SEARCH_BASE $REALM

# Start Kerberos manually on an Open Directory master
kdcsetup -a $ADMIN $REALM

# Change the global password policy of user accounts in the same domain
pwpolicy -a $ADMIN_USER -setglobalpolicy "minChars=4
     maxFailedLoginAttempts=3"

# Set the binding policy for an Open Directory master
slapconfig -setmacosxodpolicy -binding required

# Set the security policy for an Open Directory master
slapconfig -setmacosxodpolicy -cleartext blocked

# ------------------------------------------------------------------
# Securing RADIUS Service
# ------------------------------------------------------------------

# Disable RADIUS service
radiusconfig stop

# Use a custom certificate
serveradmin settings radius:eap.conf:CA_file = "/etc/certificates/$CA_CRT"
serveradmin settings radius:eap.conf:private_key_file =
     "/etc/certificates/$KEY"
serveradmin settings radius:eap.conf:private_key_password = "$PASS"
serveradmin settings radius:eap.conf:certificate_file =
     "/etc/certificates/$CERT"

# Edit RADIUS access
dseditgroup -o edit -a $USER -t user com.apple.access_radius

# View the Radius service log
tail /var/log/radius/radius.log

# ------------------------------------------------------------------
# Securing Print Service
# ------------------------------------------------------------------

# Disable Print service
serveradmin stop print

# Set administrator SACL permissions for Print service
dseditgroup -o edit -a $USER -t user com.apple.monitor_print
```

```
# Configure Kerberos for Print service
cp /etc/cups/cupsd.conf $TEMP_FILE
/usr/bin/sed "/^DefaultAuthType.*/s//DefaultAuthType Negotiate/g" $TEMP_FILE
     > /etc/cups/cupsd.conf

# View Print service logs
tail /Library/Logs/PrintService/PrintService_admin.log

# ------------------------------------------------------------------------
# Securing Multimedia Services
# ------------------------------------------------------------------------

# Disable QTSS
serveradmin stop qtss

# Configure a streaming server
serveradmin settings
     qtss:server:bind_ip_addr:_array_index:0 = "$Bind_IP_Address"

# Serve QuickTime streams over HTTP port 80
$ serveradmin settings
     qtss:server:rtsp_port:_array_index:0 = 554
     qtss:server:rtsp_port:_array_index:1 = 80
     qtss:server:rtsp_port:_array_index:2 = 8000
     qtss:server:rtsp_port:_array_index:3 = 8001

# Change the MP3 broadcast password
serveradmin settings
qtss:modules:_array_id:QTSSMP3StreamingModule:mp3_broadcast_password =
     "password"

# Create a broadcast user name and password on the streaming server
serveradmin settings
     qtss:modules:_array_id:QTSSReflectorModule:allow_broadcasts = yes

# Add a user account
qtpasswd $USER

# Adding groups
echo "$GROUP_NAME: $USER1 $USER2 $USER3" /Library/QuickTimeStreaming/Config/
     qtgroups

# Change a user password
qtpasswd $USER

# View the QTSS log
tail /Library/QuickTimeStreaming/Logs/$LOG_FILE
```

```
# ------------------------------------------------------------------
# Xgrid Service
# ------------------------------------------------------------------

# Disable Xgrid service
serveradmin stop xgrid

# Configure an Xgrid agent on the server
/usr/sbin/xgridctl agent stop


# Configure an Xgrid controller
serveradmin settings xgrid:ControllerSettings:Enabled = yes
serveradmin settings xgrid:ControllerSettings:prefs:ClientAuthentication =
     Password
serveradmin settings xgrid:ControllerSettings:ClientPassword =
     $Xgrid_Client_Password

# ------------------------------------------------------------------
# Maintaining System Integrity
# ------------------------------------------------------------------

# Validate application bundle integrity.
codesign -v $code_path

# Verify a requirement.
codesign -v -R="identifier com.apple.Mail and anchor apple" /Applications/
     Mail.app

# Install the common criteria tools software
installer -pkg CommonCriteriaTools.pkg -target /

# Enable auditing
cp /etc/hostconfig /tmp/test

if /usr/bin/grep AUDIT /etc/hostconfig
then
  /usr/bin/sed "/^AUDIT.*/s//AUDIT=-YES-/g" /tmp/test > /etc/hostconfig
else
  /bin/echo AUDIT=-YES- >> /etc/hostconfig
fi

# View logs in Server Admin
# Use tail or more to view the log files.
# The audit files are individually named based on the date.

/usr/bin/tail $AUDIT_FILE
```

Glossary

This glossary defines terms and spells out abbreviations you may encounter while working with online help or the various reference manuals for Leopard Server.

access control A method of controlling which computers can access a network or network services.

ACE Access Control Entry. An entry within the ACL that controls access rights. See **ACL**.

ACL Access Control List. A list maintained by a system that defines the rights of users and groups to access resources on the system.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined "admin" group.

administrator computer A Leopard computer onto which you've installed the server administration applications from the Mac OS X Server Admin CD.

AFP Apple Filing Protocol. A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

authentication The process of proving a user's identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user's level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

authentication authority attribute A value that identifies the password validation scheme specified for a user and provides additional information as required.

authorization The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an authentication process proves the user's identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

BIND Berkeley Internet Name Domain. The program included with Leopard Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

binding A connection between a computer and a directory domain for the purpose of getting identification, authorization, and other administrative data. (v.) The process of making such a connection. See also **trusted binding**.

biometrics A technology that authenticates a person's identity based on unique physiological or behavioral characteristics. Provides an additional factor to authentication. See **two-factor authentication**.

Bonjour A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. Formerly called "Rendezvous," this proposed Internet standard protocol is sometimes referred to as "ZeroConf" or "multicast DNS."

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

buffer caching Holding data in memory so that it can be accessed more quickly than if it were repeatedly read from disk.

cache A portion of memory or an area on a hard disk that stores frequently accessed data in order to speed up processing times. Read cache holds data in case it's requested by a client; write cache holds data written by a client until it can be stored on disk. See also **buffer caching**, **controller cache**, **disk cache**.

certificate Sometimes called an "identity certificate" or "public key certificate." A file in a specific format (Leopard Server uses the x.509 format) that contains the public key half of a public-private keypair, the user's identity information such as name and contact information, and the digital signature or either a *certificate authority* (CA) or the key user.

Certificate Authority An authority that issues and manages digital certificates in order to ensure secure transmission of data on a public network. See also **public key infrastructure and certificate.**

cluster A collection of computers interconnected in order to improve reliability, availability, and performance. Clustered computers often run special software to coordinate the computers' activities. See also **computational cluster**.

computational cluster A group of computers or servers that are grouped together to share the processing of a task at a high level of performance. A computational cluster can perform larger tasks than a single computer would be able to complete, and such a grouping of computers (or "nodes") can achieve high performance comparable to a supercomputer.

controller In an Xsan storage area network, short for metadata controller. In RAID systems, controller refers to hardware that manages the reading and writing of data. By segmenting and writing or reading data on multiple drives simultaneously, the RAID controller achieves fast and highly efficient storage and access. See also **metadata controller**.

controller cache A cache that resides within a controller and whose primary purpose is to improve disk performance.

cracker A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to hacker.

crypt password A type of password that's stored as a hash (using the standard UNIX encryption algorithm) directly in a user record.

daemon A program that runs in the background and provides important system services, such as processing incoming email or handling requests from the network.

decryption The process of retrieving encrypted data using some sort of special knowledge. See also **encryption**.

deploy To place configured computer systems into a specific environment or make them available for use in that environment.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a lease period—the length of time the client computer may use the address.

directory Also known as a folder. A hierarchically organized list of files and/or other directories.

disk cache A cache that resides within a disk. See also **cache**, **controller cache**.

disk image A file that, when opened, creates an icon on a Mac OS X desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

DoS attack Denial of service attack. An Internet attack that uses thousands of network pings to prevent the legitimate use of a server.

drop box A shared folder with privileges that allow other users to write to, but not read, the folder's contents. Only the owner has full access. Drop boxes should be created only using AFP. When a folder is shared using AFP, the ownership of an item written to the folder is automatically transferred to the owner of the folder, thus giving the owner of a drop box full access to and control over items put into it.

Dynamic Host Configuration Protocol See **DHCP**.

EFI Extensible Firmware Interface. Software that runs automatically when an Intel-based Macintosh first starts up. It determines the computers hardware configuration and starts the system software.

encryption The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications. See also **decryption**.

Ethernet A common local area networking technology in which data is transmitted in units called packets using protocols such as TCP/IP.

file server A computer that serves files to clients. A file server may be a general-purpose computer that's capable of hosting additional applications or a computer capable only of serving files.

firewall Software that protects the network applications running on your server. IP firewall service, which is part of Leopard Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

firmware Software that's stored in read-only memory (ROM) on a device and helps in starting up and operating the device. Firmware allows for certain changes to be made to a device without changing the actual hardware of the device.

FTP File Transfer Protocol. A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

hacker An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

hash (noun) A scrambled, or encrypted, form of a password or other text.

host Another name for a server.

host name A unique name for a computer, historically referred to as the UNIX hostname.

HTTP Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. The HTTP protocol provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

ICMP Internet Control Message Protocol. A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

image See **disk image**.

IMAP Internet Message Access Protocol. A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local computer. Mail remains on the server until the user deletes it.

installer package A file package with the filename extension .pkg. An installer package contains resources for installing an application, including the file archive, Read Me and licensing documents, and installer scripts.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

IPv4 See **IP**.

IPv6 Internet Protocol version 6. The next-generation communication protocol to replace IP (also known as IPv4). IPv6 allows a greater number of network addresses and can reduce routing loads across the Internet.

JBoss A full-featured Java application server that provides support for Java 2 Platform, Enterprise Edition (J2EE) applications.

KDC Kerberos Key Distribution Center. A trusted server that issues Kerberos tickets.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Leopard Server uses Kerberos v5.

kernel The part of an operating system that handles memory management, resource allocation, and other low-level services essential to the system.

L2TP Layer Two Tunnelling Protocol. A network transport protocol used for VPN connections. It's essentially a combination of Cisco's L2F and PPTP. L2TP itself isn't an encryption protocol, so it uses IPSec for packet encryption.

LAN Local area network. A network maintained within a facility, as opposed to a WAN (wide area network) that links geographically separated facilities.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

managed network The items managed clients are allowed to "see" when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a "network view."

metadata controller The computer that manages metadata in an Xsan storage area network.

mutual authentication Also known as two-way authentication. A type of authentication in which two parties authenticate with each other. For example, a client or user verifies their identity to a server, and that server confirms its identity to the client or user. Each side has the other's authenticated identity.

NAT Network Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications.

NetBoot server A Leopard Server on which you've installed NetBoot software and have configured to allow clients to start up from disk images on the server.

Network File System See **NFS**.

network view See **managed network**.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

node A processing location. A node can be a computer or some other device, such as a printer. Each node has a unique network address. In Xsan, a node is any computer connected to a storage area network.

NTP Network time protocol. A network protocol used to synchronize the clocks of computers across a network to some time reference clock. NTP is used to ensure that all the computers on a network are reporting the same time.

object class A set of rules that define similar objects in a directory domain by specifying attributes that each object must have and other attributes that each object may have.

offline Refers to data that isn't immediately available, or to devices that are physically connected but not available for use.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, or Active Directory protocols; BSD configuration files; and network services.

Open Directory master A server that provides LDAP directory service, Kerberos authentication service, and Open Directory Password Server.

Open Directory password A password that's stored in secure databases on the server and can be authenticated using Open Directory Password Server or Kerberos (if Kerberos is available).

Open Directory Password Server An authentication service that validates passwords using a variety of conventional authentication methods required by the different services of Leopard Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

partition A subdivision of the capacity of a physical or logical disk. Partitions are made up of contiguous blocks on the disk.

PDC Primary domain controller. In Windows networking, a domain controller that has been designated as the primary authentication server for its domain.

permissions Settings that define the kind of access users have to shared items in a file system. You can assign four types of permissions to a share point, folder, or file: read/write, read-only, write-only, and none (no access). See also **privileges**.

phishing An attempt to masquerade as a trusted organization or individual to trick others into divulging confidential information.

PKI Public Key Infrastructure. A mechanism that allows two parties to a data transaction to authenticate each other and use encryption keys and other information in identity certificates to encrypt and decrypt messages they exchange.

POP Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

portable home directory A portable home directory provides a user with both a local and network home folder. The contents of these two home folders, as well as the user's directory and authentication information, can be automatically kept in sync.

POSIX Portable Operating System Interface for UNIX. A family of open system standards based on UNIX, which allows applications to be written to a single target environment in which they can run unchanged on a variety of systems.

print queue An orderly waiting area where print jobs wait until a printer is available. The print service in Leopard Server uses print queues on the server to facilitate management.

private key One of two asymmetric keys used in a PKI security system. The private key is not distributed and usually encrypted with a passphrase by the owner. It can digitally sign a message or certificate, claiming authenticity. It can decrypt messages encrypted with the corresponding public key. Finally, it can encrypt messages that can only be decrypted by the private key.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

protocol A set of rules that determines how data is sent back and forth between two applications.

proxy server A server that sits between a client application, such as a web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

public key One of two asymmetric keys used in a PKI security system. The public key is distributed to other communicating parties. It can encrypt messages that can be decrypted only by the holder of the corresponding private key, and it can verify the signature on a message originating from a corresponding private key.

public key certificate See **certificate**.

public key infrastructure A secure method of exchanging data over an insecure public network, such as the Internet, by using public key cryptography.

QTSS QuickTime Streaming Server. A technology that lets you deliver media over the Internet in real time.

record type A specific category of records, such as users, computers, and mounts. For each record type, a directory domain may contain any number of records.

recursion The process of fully resolving domain names into IP addresses. A nonrecursive DNS query allows referrals to other DNS servers to resolve the address. In general, user applications depend on the DNS server to perform this function, but other DNS servers do not have to perform a recursive query.

rogue computer A computer that is set up by an attacker for the purpose of infiltrating network traffic in an effort to gain unauthorized access to your network environment.

root An account on a system that has no restrictions. System administrators use this account to make changes to the system's configuration.

router A computer networking device that forwards data packets toward their destinations. A router is a special form of gateway which links related network segments. In the small office or home, the term router often means an Internet gateway, often with Network Address Translation (NAT) functions. Although generally correct, the term router more properly refers to a network device with dedicated routing hardware.

RSA Rivest Shamir Adleman algorithm. A public key encryption method that can be used both for encrypting messages and making digital signatures.

SACL Service Access Control List. Lets you specify which users and groups have access to specific services. See **ACL**.

schema The collection of attributes and record types or classes that provide a blueprint for the information in a directory domain.

server A computer that provides services (such as file service, mail service, or web service) to other computers or network devices.

shadow password A password that's stored in a secure file on the server and can be authenticated using a variety of conventional authentication methods required by the different services of Leopard Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

shared secret A value defined at each node of an L2TP VPN connection that serves as the encryption key seed to negotiate authentication and data transport connections.

single sign-on An authentication strategy that relieves users from entering a name and password separately for every network service. Leopard Server uses Kerberos to enable single sign-on.

smart card A portable security device that contains a microprocessor. The smart card's microprocessor and its reader use a mutual identification protocol to identify each other before releasing information. The smart card is capable of securely storing passwords, certificates, and keys.

SMB Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB to provide access to servers, printers, and other network resources.

SMTP Simple Mail Transfer Protocol. A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SNMP Simple Network Management Protocol. A set of standard protocols used to manage and monitor multiplatform computer network devices.

Spotlight A comprehensive search engine that searches across your documents, images, movies, PDF, email, calendar events, and system preferences. It can find something by its text content, filename, or information associated with it.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

standalone server A server that provides services on a network but doesn't get directory services from another server or provide directory services to other computers.

static IP address An IP address that's assigned to a computer or device once and is never changed.

streaming Delivery of video or audio data over a network in real time, as a stream of packets instead of a single file download.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration. See also **IP subnet**.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

ticket, Kerberos A temporary credential that proves a Kerberos client's identity to a service.

trusted binding A mutually authenticated connection between a computer and a directory domain. The computer provides credentials to prove its identity, and the directory domain provides credentials to prove its authenticity.

tunneling A technology that allows one network protocol to send its data using the format of another protocol.

two-factor authentication A process that authenticates through a combination of two independent factors: something you know (such as a password), something you have (such as a smart card), or something you are (such as a biometric factor). This is more secure than authentication that uses only one factor, typically a password.

UDP User Datagram Protocol. A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

VPN Virtual Private Network. A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

WAN Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

weblog A webpage that hosts chronologically ordered entries. It functions as an electronic journal or newsletter. Weblog service lets you create weblogs that are owned by individual users or by all members of a group.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

zone transfer The method by which zone data is replicated among authoritative DNS servers. Slave DNS servers request zone transfers from their master servers to acquire their data.

Index

A

access
- ACEs 73
- ACLs 205, 260, 395
- application 300, 301, 305
- connection control 261–265
- Directory Access 185
- file 358
- Keychain Access Utility 197
- media 314
- passwords 357, 360
- playlists 358
- printing 348
- QTSS 355, 357, 358, 361
- remote installation 40
- restricting NetBoot 328
- restricting Software Update 331
- SACLs 205, 248
- share point 180–183
- Universal Access 324
- user 30–32, 288, 357, 360
- weblogs 294–295
- website 288, 317–319
- wireless users 343
- *See also* ACLs; IMAP;LDAP; permissions

access control entries. *See* ACEs
access control lists. *See* ACLs
access warnings 90–93
- *See also* permissions

accounts
- administrator 94–95, 97–100, 185
- authentication 358
- authentication setup 103–112
- creating secure 97–100
- credential storage 107–??
- directory domains 100–103
- group 187–188, 360, 361
- mobile 101, 314–316
- nonadministrator user 94–95
- preferences 116–118
- types 94
- user 360, 361
- *See also* user accounts; Workgroup Manager

ACEs (access control entries) 73, 155
Acknowledgments 25
ACLs (access control lists)
- keychain services 107
- mail service access 260
- permissions 73, 151, 155–156, 181
- print service access 348
- SACLs 205, 395

Active Directory 102–103, 180
activity analysis tools 384–387
Address Book 101
addresses. *See* email addresses; IP addresses; NAT
address translation 356
administrator 73
- accounts for 185
- auditing tools 378–384
- directory domain 98, 179
- passwords for 339, 401
- privileges of 73, 369

administrator account 94–95, 97–100
administrator computer 37
adult websites, access control 317
AFP (Apple Filing Protocol) service
- authentication 276
- configuration 278–279
- share points 183

agents
- authentication 364, 365
- controllers 367
- functions of 363
- setup 367

agents, Xgrid 366–368
AirPort, disabling 77
AirPort Base Station
- and RADIUS 344

anonymous access, FTP 280
antivirus tools. *See* virus screening
`any-user` tag 359
APOP (authenticated POP) 255
appearance preferences 119–120
Apple Filing Protocol service. *See* AFP

Apple Remote Desktop. *See* ARD
Apple Software Restore. *See* ASR
AppleTalk 350
applications
 access control 31, 300, 301
 legacy access 305
 securing 33, 89
applications, user access to
 See also specific applications
ARD (Apple Remote Desktop) 203–204
ARD. *See* Apple Remote Desktop
ARP (Address Resolution Protocol) spoofing 230
assistive devices 150
attributes
 ACL 182
 authentication 400
 configuration 373
audio recording devices, disabling 80
audit_class file 383
audit_control file 383
audit_event file 383
audit_user file 383
audit_warn file 383
auditing tools 378–384
`auditreduce` tool 381–382
`audit` tool 380–381
authenticated POP. *See* APOP 253
authentication
 Active Directory 102
 AFP 276
 attributes 400
 vs. authorization 30
 cached 396
 credential-based 395
 definition 394
 Directory Access 101–102
 directory services 179
 EAP 218, 344
 file services 278–280
 FTP 276
 iCal service 243
 IMAP 256
 Kerberos 214, 218, 255, 257, 258, 349, 399
 methods 335, 396
 NFS 276
 options 365, 366, 367
 passwords 55, 291, 292, 365, 366, 368
 POP 255
 QTSS 357, 358, 360
 Server Admin 192
 SMB/CIFS-related 276
 SMTP 262, 263
 SSH 209–211
 strengthening methods 103–106
 system preferences 112
 user 394, 399–401, 402
 VPN 214
 WebDAV 289
 Workgroup Manager 179–180
 See also keychain services; passwords; RADIUS
authentication authority attributes 400
authorization 30–35, 98, 394
 See also authentication
authorization rights 374–375, ??–375
`AuthScheme` keyword 359
automatic actions, disabling 121
Automatic Unicast 357

B

backups 177–178
BannerSample file, modifying 92
bayesian filters 266
Berkeley Software Distribution. *See* BSD
Bill of Materials file 74
BIND (Berkeley Internet Name Domain) 225, 226, 229
binding 340
biometrics-based authentication 106
blacklisted servers 261, 263
blogs 294–295
blog service 294, 295
Bluetooth preferences 78, 120–121
Bonjour browsing service 240
`boot` command 88
boot image, definition 326
broadcasting, MP3 357
browsers, network 240
BSD (Berkeley Software Distribution) 27, 385
bundle IDs 300

C

CA. *See* certificate authority
cached authentication 396
cache poisoning
 DNS 228
cameras 81, 251
`cat` tool 352
CDs 41
CDs, preferences 121
CDSA (Common Data Security Architecture) 27
CERT (Computer Emergency Response Team) 27
Certificate 192, 193
Certificate Authority (CA)
 creating 200
 requesting certificates from 194
certificate authority (CA)
 See also certificates
 creating 196
 creating certificates from 199
 distributing to clients 200
 introduction 190

overview 191
requesting certificates from 191, 199, 255
Certificate Manager 192, 194
certificates
certificate authority 196, 200
creating 199
deleting 195
editing 195
FileVault 164
iChat server 246
identities 191
importing 194
IPSec 214
mail service 254–255
management of 33–34
managing 195
Open Directory 337
overview 189–200
POP 256
private keys 190
public keys 190, 376–377
renewing 196
requesting 191–193, 255
root 196
self-signed 191, 194, 195
and Server Admin 192–??
SSL 244, 248, 291
web service 292
Certificate Signing Request. *See* CSR 253
CGI (Common Gateway Interface) scripts
enabling 287
chat service 245–249
CIFS (Common Internet File System). *See* SMB/CIFS
ClamAV 265, 269
clean installation 42
clients
access control 357
authentication 365
certificates 200
earlier operating systems 214
group accounts 187–188
groups 360, 361
and SSL 254
See also client computers; users
`codesign` command 377–378
collaboration services
group accounts 187–188
See also mail service; specific file services
command 358
command-line interface
access warnings 93
Certificate Authority 198
erasing files 170–171
installing from 59–62
options 358
security 276
startup security setup 89
command-line tools
erasing disks 54
installing server software 59
log viewing 292
passwords 340
`sudo` 239
viewing logs 352
command-line tools, Firewall service 388
command mode startup 88
Common Criteria Tools 378
Common Data Security Architecture. *See* CDSA
Common Security Service Manager. *See* CSSM
Common UNIX Printing System. *See* CUPS
Computer Emergency Response Team. *See* CERT
computer groups 188
computer name 205
computers
host name 140
idle status 367
name 205
See also portable computers
computers, administrator 37
concatenated RAID set 51
configuration
access control 348
agents 367
batch setup for multiple servers 68
controller 368
DHCP 38
Firewall service 233, 234
iChat 245–247
incoming mail 257
interactive 63, 66, 67, 68
Kerberos 335
keychain services 108–110
Mac OS X Server file changes 226
overview 253
RADIUS 344
remote server 64, 67, 68
share points 180
SSH 208–209
VPN 215, 216
See also Mailman setup
configuration files, SSH 209
Console application 385
contacts search policy 101–102, 185
controllers
and agents 367
nodes 364
setup 368
controllers, Xgrid 368
CRAM-MD5 authentication 257, 258
credential-based authentication 374–375, 395
credential storage 107–??
crypt passwords

definition 396
encryption 186, 400
CSR (Certificate Signing Request) 189, 191–193, 194, 199
CSSM (Common Security Service Manager) 29
CUPS (Common UNIX Printing System) 347
curfews on computer use 320
Cyrus mail service 253

D

Dashboard preferences 130–131, 301, 303
databases 179
data security 82–83, 151–171, 174–175, 177–178
data transport encryption 244
Date & Time preferences 123–124, 205
decryption. *See* encryption
Desktop preferences 125–126
DHCP (Dynamic Host Configuration Protocol) service 38, 222, 340
DHX authentication 396
dictionaries
rights 371, ??–375
Dictionary, hiding profanity in 318
digest authentication 243, 358
digest authentication, WebDAV 289
digital signatures 300, 301, 376–377
directories. *See* directory services; domains, directory; folders
Directory Access 101–102, 185
directory domain administrator 98, 179
directory services
Active Directory 102–103, 180
directory domains 39, 100–103
Open Directory 102
organization of 179
overview 333
standalone server 65
See also domains, directory; Open Directory
directory services, Open Directory 343
discovery, service 101
disk images
encrypting 34, 166–168
installing with 43, 46
read/write 166
disks
command-line management of 54
erasing free space 53
installation preparation 47–53
mirroring 51
partitions 42, 49, 50, 52, 53
permissions for 72–74
quotas 186
startup 147–148
Disk Utility 34, 49, 52, 53, 74, 170, 171
`diskutil` tool 52, 54
display mirroring 127
Displays preferences 127
distributed computing architecture 363–368
DNS (Domain Name System) service
BIND 225, 226, 229
IP addresses 229
recursion 227, 230
securing server 227, 229
setup 38
Dock preferences 127, 306–307
documentation 22–25
Domain Name System. *See* DNS
domains, directory
Active Directory 180
administrator for 98, 179
binding of 340
databases 179
LDAP 218
management of 179
overview 100–103
setup 39
See also LDAP; Open Directory
DoS attack (denial of service) 229, 401
duplication of settings 185
DVDs 41, 313–314
DVDs, preferences 121
Dynamic Host Configuration Protocol (DHCP) 222

E

EAP (Extensible Authentication Protocol) 344
EAP-SecurID authentication 218
EFI (Extensible Firmware Interface) 86, 148
email. *See* mail service
Enabling 156
encryption
AFP 278
certificates 190
crypt passwords 186, 400
disk images 34
FileVault 162–166, ??–168
mail service 255
network configuration 219
ports 248
secure virtual memory 174–175
SSH 202, 219, 277–280
SSL 290
Time Machine 177–178
VPN protocols 214
See also SSL
Energy Saver preferences 128–129
erasing data permanently 36, 59, 169–171
error messages. *See* troubleshooting
Everyone permission level 152
Exposé & Spaces preferences ??–131
Exposé and Spaces preferences 130–??

Extensible Authentication Protocol. *See* EAP
Extensible Firmware Interface. *See* EFI

F

Fast User Switching 176, 312
fax preferences 135–137
files
 access control 358
 backup of 177–178
 encryption 162–168, 219
 erasing 36, 59, 169–171
 OpenSSL 199
 permissions 151–154, 157
 qtaccess 358
 qtgroups 359
 qtusers 359
 security 174–175
 shared secret 190
 transferring 213
file services
 authentication 278–280
 disabling 276
 FTP 183, 280–282
 NFS 282
 See also AFP; FTP; NFS; share points
file sharing 274–275
file systems
 choosing 47
 erasing data 169
 securing 37
File Transfer Protocol. *See* FTP
FileVault 33–34, 75, 162–166, 315
FileVault master keychain 164
filters
 blacklisted mail senders 261, 263
 junk mail 265, 267
 virus 261, 269, 271
Finder preferences 308–309
fingerprints, server 211
firewalls 265, 354, 355, 356
 See also Firewall service
Firewall service 388
 access control 32–33
 advanced rules setup 234
 introduction 231
 logs 236
 and NAT 237
 services settings 233
 settings 39
 starting 232
 stealth mode 235
FireWire 83, 148
FireWire Bridge Chip GUID 148
firmware, open password 37, 87–89, 148
flags for files and folders 154–155
folders
 flags for 154–155
 group 187
 home 100, 161–164, ??–166, 183, 314
 permissions for 161–162
 website 287
free disk space, erasing 171, 172
Front Row 301, 304
FTP (File Transfer Protocol) service 183, 276, 277, 280–282
full mode startup 88

G

GID (group ID) 186
global file permissions 157
global password policy 339
grids, computational 363
grids, computer 363
group accounts 187–188, 360, 361
 See also groups
`group filename` keyword 359
group folders 187
`groupname` keyword 359
groups
 blog service 294, 295
 configuration 187–188
 permissions 152
guest accounts
 permissions 152, 275

H

hard drive 75
hardware, protection of 75
hardware requirements 51
hash, password 396
help, using 22
helper applications 305
HFS+J volume 48
HFSX volume 48
HISEC (Highly Secure) templates 102, 180
home folders 101, 161–166, 180, 183, 314
hostconfig entries 379
host name 140, 205
hosts. *See* servers
HTTP (Hypertext Transfer Protocol) 290, 354, 356

I

iCal service 242–245
iChat service 245–249
identity certificates. *See* certificates
IETF (Internet Engineering Task Force) standard 354
images. *See* disk images; NetBoot; Network Install
IMAP (Internet Message Access Protocol)
 authentication 256–257
 log 270, 273

importing certificates 194
incoming mail
 security 254
 setup 257
installation
 administrator computer 37
 auditing tools 378
 command line 59–62
 command-line method 59
 directory connections 39
 with disk images 43, 46
 disk preparation 47–53
 from earlier OS versions 38
 from removable media 41–42
 identifying servers 54
 installer packages 141
 interactive 55, 57, 58
 multiple server 62
 network services setup 38
 overview 36–37
 permission repair 72–74
 remote access 38, 40, 54, 57
 server installation disc 38
 server software 39, 41–42, 59, 69–72
 starting up for 39, 42, 46
 updating 63
 upgrading 63
installer packages 71, 141
`installer` tool 59, 62
install image, definition 326
instant messaging 245–249
Intel-based Macintosh 37, 86
internal Software Update server 70
International preferences 131
Internet Message Access Protocol. *See* IMAP
Internet Printing Protocol. *See* IPP
Internet security
 MobileMe preferences 114–116
 sharing 139–140
 wireless connections 79
IP addresses
 DHCP 222
 DNS recursion 226–227
 DNS service 229
 and firewalls 39
 groups 232
 IPv6 addressing 133
 IPv6 notation 221–222
 port forwarding 239
 QTSS 355
 and recursion 227
 remote server installation 40, 54
 servers on different subnets 64
IPFilter service. *See* Firewall service
IPFW2 software 388
IP masquerading. *See* NAT
IPP (Internet Printing Protocol) 347
IPSec (IP security) 214, 215
IPv6 addressing 133, 221–222
iSight, disabling 81
ISP (Internet service provider) 214

J

Jabber instant messaging project 245–249
jobs 363
journaling, file system 48
junk mail screening
 connection control 261–265
 filters 265, 267
 log 270, 273
 overview 261

K

KDC (Kerberos Key Distribution Center). *See* Kerberos
Kerberos
 Active Directory 102
 authentication 104–105, 214, 243, 255–258, 399
 features 395, 401, 402
 Open Directory 180
 passwords 401
 print service 349
 setup 335
 users 336, 402
 WebDAV 289
 Xgrid administration 365
kernel extensions, removing 84
key-based SSH connection 209–211
Keyboard & Mouse preferences 132
Keychain Access 107
Keychain Access Utility 197
keychain services 29, 33, 107–??, 164

L

L2TP/IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) 35, 214, 215
LANs (local area networks) 213, 282
layered security architecture 28
Layer Two Tunneling Protocol, Secure Internet protocol (L2TP/IPSec). *See* L2TP/IPSec
LDAP (Lightweight Directory Access Protocol) service
 advanced settings 333
 configuration 102
 overview 333
 security 337, 341, 394
 VPN 218
 See also attributes; mappings; object classes; trusted binding
LDAPv3 access 179, 333
Legacy preferences 301, 305
Lightweight Directory Access Protocol. *See* LDAP

Line Printer Remote (LPR) printing 350
local area networks (LANs) 282
local directory domains
password types 394, 396
local installation 41–42
local system logging 386
local versus network home folders 180
locking folders 154
login
access warnings 90–93
keychain 108
preferences 310–313
preferences overview 310
remote 202
security measures 116–118
login scripts 311
logs
audit 384
Blog service 296
configuration 385–387
Firewall service 236
iChat 249, 250, 252
mail service 270, 273
MySQL service 298
NetBoot 328
print service 351
QTSS 361
RADIUS 346
Software Update service 332
web service 292
LPR (Line Printer Remote) printing 350

M

MAC (media access control) addresses 54
Mach 27
Mac OS X
installation considerations 37
Open Directory passwords 395
upgrading from 63
Mac OS X Server
agent setup 367
authentications supported 335, 402
configuration file changes 226
trusted binding 340
mail service
certificates 254–255
disabling 253
group settings 187
logs 270, 273
security 254, 255
virus filtering 271
mail transfer agent. *See* MTA
managed accounts 185–188
managed preferences
Dashboard 130–131, 301, 303
Date & Time 123–124, 205
Desktop 125–126
Displays 127
Dock 127, 306–307
Energy Saver 128–129
Exposé & Spaces ??–131
Exposé and Spaces 130–??
Finder 308–309
Front Row 301, 304
International 131
Keyboard & Mouse 132
Legacy 301, 305
Login 310–313
Media Access 313–314
MobileMe 114–116
Mobility 314–316
Network 133–134, 316–317
overview 300
Parental Controls 317, 318, 319
Print & Fax 135–137
Printing 321–322
Security 138
Sharing 139–140, 203–??
Software Update 141, 322
Sound 142
Spotlight 145–147
Startup Disk 147–148
System 323–324
System Preferences 323, 324
Time Machine 177–178
Universal Access 150, 324
See also preferences
managed user accounts 94, 185–188
mandatory access controls 30–32
man-in-the-middle attacks 212
Media Access 313–314
`message` keyword 359
microphones, disabling 80
Microsoft Windows compatibilities 155
mirroring, disk 51
mobile accounts 101, 214, 314–316, 401
MobileMe preferences 114–116
Mobility preferences 314–316
movies, QuickTime cache
See also streaming media
MP3 files 357
MS-CHAPv2 authentication 217, 335
MTA (mail transfer agent) 253
multimedia 353–361
MySQL service 296, 298

N

name server. *See* DNS
naming conventions, computers 205
NAT (Network Address Translation)

and Firewall service 237
introduction 237
NetBoot service 46, 326–328
NetInstall 46
Network Address Translation. *See* NAT
network-based directory domains 100–103
network-based keychains 111–??
Network File System. *See* NFS
network install image 148
Network preferences 316–317
networks
client connections 35
preferences 317
views troubleshooting 185
network services
DHCP 38, 222
DNS 38
FileVault limitations 162, 166
home folders 179
installation 38
IPv6 addressing 221–222
keychains 111
managed users 97
NTP 201
preferences 133–134, 316–317
sharing 139–140
sleep mode security 128
VPN 213–218
wireless preferences 120–121
See also IP addresses
network settings
firewall consideration 356
Network Time Protocol. *See* NTP
`newsyslog` command 386
NFS (Network File System)
file sharing 184, 275, 282
security 276
share points 183–184, 274, 277
nodes, controller 364
nodes, directory. *See* domains, directory
nonadministrator user accounts 94–95
NT Domain services 283–284, 350
NTLM authentication 335
NTP (network time protocol) 201
`nvram` tool 89

O

Open Directory
access control 358
Active Directory 179
binding policy 340
configuration 102, 334–340
definition 179
DNS recursion 226
and Kerberos 395
options settings 340
overview 333
password type 186, 338
and RADIUS 343
and SACLs 205
security policy 341
See also domains, directory
Open Directory master
authentication 365
binding 340
security policy 341
setup 39
Open Directory Password Server
access control 344
authentication 334, 395
password policy 401
Open Firmware Password 89
Open Firmware password 37, 87–89, 148
open source modules
Apache 285
Jabber 246
Kerberos 243, 289
OpenSSL 199
open source software 27–28
option 95, DHCP 340
Others user category 274
outgoing mail, security 254
Overview 163
owner permission 152

P

Parental Controls 97, 317, 318, 319
partitions, disk 42, 49, 50–53
Password Assistant 103–104, 117
passwords
administrator 65, 339, 401
Apache 292
authentication 365, 366, 368
authentication set 103
authentication setup 255–256
changing 116–118
command-line tools 89
crypt 186, 400
firmware 37, 87–89, 148
hash 396
keychain 108
master FileVault 163–164, ??–166
Open Directory 395, 400
policies 339, 401
preset 55
security 398–399
vs. single sign-on 401
SSL passphrase 291
Startup Disk preferences 148
streaming media 357

tokens 106
types 394, 395, 396
user account 360
VPN 214
Windows domain 400
Password Server. *See* Open Directory Password Server
PDFs, encrypting 168
permissions
access 27
ACLs 73, 181, 348
administrator 369
disk 74
folders 161–162
guest 275
manipulating 154
overview 151–157
share points 181–183
types 274
user 186–188, 288, 292
viewing 152
WebDAV 288
physical access, securing 75
physical computers
hardware security 75
piggybacking, service 230
PKI (public key infrastructure) 189, 190
See also certificates
playlists
accessing 358
QTSS 353
plist files 239
Podcast Producer service 251–252
policy database 371–375
POP (Post Office Protocol) 256, 270, 273
port 355
portable computers
FileVault 162
keychains 111–??
mobile accounts 101, 214, 314–316
portable files, encrypting 166–168
portable keychains 111
port forwarding 239
ports
encryption 248
QTSS 354–356
and SSL 290
VPN 215
POSIX (Portable Operating System Interface) 73, 151–157
Postfix transfer agent 253
Post Office Protocol. *See* POP
PPTP (Point-to-Point Tunneling Protocol) 214, 216
`praudit` tool 382–383
preferences
accounts 116–118
appearance 119–120
Bluetooth wireless 120–121
CDs 121, 313–314
DVDs 121
fax 135–137
login 310–313
overview 112–113
QuickTime 137–138
screen saver 125–126
speech recognition 143
time 123–124, 205
See also managed preferences
presets 185
primary zone, DNS 228
Print & Fax preferences 135–137
print service
access control 321–322, 348
command-line tools 352
security 347–352
private key 190, 191
private key cryptography 290
privileges, administrator 73, 369
See also permissions
problems. *See* troubleshooting
profanity, hiding 318
profiling, DNS service 229
protocols
EAP 344
file services 277
HTTP 290
LDAP 218
network service 38
POP 256, 270, 273
RTP 354
RTSP 354
TCP 233
VPN 214, 215, 216, 218
See also specific protocols
proxy server settings 316–317, 355
public key certificates 211
public key certificates. *See* certificates
public key cryptography 290, 376–377
public key infrastructure. *See* PKI
`pwpolicy` command 106
`pwpolicy` tool 340

Q

qtaccess file 358
qtgroups file 359
`qtpasswd` tool 358
QTSS. *See* QuickTime Streaming Server
qtusers file 359
Quarantine 32
queues, print
creating 350

logs 351
QuickTime cache 137
QuickTime preferences 137–138
QuickTime Streaming Server (QTSS) 353–361
quotas, disk space 186

R

RADIUS (Remote Authentication Dial-In User Service)
introduction 343
RAID (Redundant Array of Independent Disks) 51, 52
read/write disk images 166
Really Simple Syndication. *See* RSS
realms. *See* Kerberos; WebDAV; websites, accessing
recent items list 119–120
recursion, DNS 226–227, 230
relays, access control 358
Remote Apple Events 204, 220
Remote Authentication Dial-In User Service (RADIUS). *See* RADIUS
Remote Login 207–208
remote servers
accessing 40
configuration 64, 67, 68
identifying 54
installing from or to 38, 40, 54, 57
login 202
system logging 386
removable media
FileVault limitations 162, 166
installation from 41–42
preferences 313–314
removable media, accessing 314
requirements
hardware 51
software 38
rights dictionary 371–373
right specifications 371–373
root certificate 196
root permissions 86, 98–99
RSA SecurIDs 218
RTP (Real-Time Transport Protocol) 354
RTSP (Real-Time Streaming Protocol) 354
rules 373

S

SACLs (service access control lists) 205, 248, 279, 282, 348, 395
sandboxing 31
scp tool 207
screening
virus 271
See also filters
screen saver preferences 125–126
searching
Spotlight 287
searching preferences 145–147
Secure Empty Trash command 171
secure notes 107
Secure Shell. *See* SSH
Secure Sockets Layer. *See* SSL
Secure Transport 29
SecurID 218
security 174–175
ACLs 348
authentication 243
best practices 274
certificates 337
DNS 227, 229
firewall 265
firewalls 354, 355, 356
Firewall service 39
installation 39
IPSec 214, 215
LDAP 337, 341, 394
NetBoot service 327
network 276
overview 254
passwords 255–256, 357, 360
print service 349
QTSS 354, 355, 356
server policy settings 341
service level 205
SSH 40, 41
SSL 190–192, 246–248, 254–259, 290, 337
tools 242, 244
VPN 214
websites 290, 292
wiki 249
See also access; authentication; permissions
security architecture overview 27–29
security-mode environment variable 89
security-password environment variable 89
Security preferences 138–??
self-signed certificates 191, 194, 195, 255
serial number, server 41
Server Admin
access control 212, 260, 275, 348
as administration tool 285
authentication 192, 217
certificates 194
opening 192
overview 189, 192
server status 226
Server Assistant 57, 63
Server Message Block/Common Internet File System. *See* SMB/CIFS
server mining 228
servers
binding to 340
blacklisted 261, 263
installation 69–72

naming 205
proxy 316–317, 355
securing DNS 227, 229
security policy 341
serial numbers for 41
SMTP 262
startup 39, 46
See also Apache web server; remote servers; websites
server side includes. *See* SSI
server software 41–42, 72
service access control lists. *See* SACLs
services, security 205
setup procedures. *See* configuration; installation
SFTP (Secure File Transfer Protocol) 213, 277–280
`sftp` tool 183, 207
shadow passwords
definition 396
features 400
shared files. *See* file sharing
shared resources
printers 135
user accounts 95
shared secret files 214
share points
configuration 180–183
home folders 180
NFS 274, 283
setup 180
Sharing preferences 139–140, 203–??
Simple Finder 309
Simple Network Management Protocol (SNMP) 202
single sign-on (SSO) authentication 105, 365, 401
single-user mode 86
sleep mode, securing 128–129
sleep settings, securing 307
smart cards 33–34, 105, 111, 186, 403
SMB/CIFS (Server Message Block/Common Internet File System) protocol
authentication 276
enabling 283–284
printing 350
security overview 278
share points 183
SMTP (Simple Mail Transfer Protocol) 261–265, 270, 273
SNMP (Simple Network Management Protocol) 202
Software Update service
clients 331
configuration 322
disabling 330
overview 331
preferences 141
settings 331
starting 330, 343
updating 69–71
Sound preferences 142
sources 279
sparse images 166
speech recognition preferences 143
spoofing
ARP 230
Spotlight preferences 145–147
Spotlight searching 287
`srm` command 170–171
SSH (secure shell host) 40, 41, 202, 207–213, 219, 280
`sshd` daemon 207
`ssh` tool 208
SSI (server side includes) 287
SSL 257
SSL (Secure Sockets Layer)
certificates 190–192, 196, 247, 248
iCal service 244
iChat service 246
mail service 254–260
Open Directory 337–338
overview 29
web service 290
standalone server 65
standard user accounts 94
startup, securing 86
Startup Disk preferences 147–148
stealth mode, Firewall service 235
streaming media 353–361
striping 51
subnets 64
`sudo` tool 98–101, 239, 369
`su` tool 99
synchronization 114–116
mobile account data 314
time 201
`syslogd` configuration file 385
system administrator (root) account 98–101
System Preferences 323–324
See also managed preferences
system preferences. *See* preferences
system software 69–72

T

`tail` tool 352
target disk mode 148
tasks 363
TCP (Transmission Control Protocol) 231, 233, 354
third-party applications 131, 138
ticket-based authentication 102
time limits on computer use 320
Time Machine 31, 149, 177–178
time settings 123–124
time synchronization 201, 202
time zone settings 205

TLS (Transport Layer Security) protocol
tokens, digital 105–106
Transmission Control Protocol (TCP) 231
Transport Layer Security protocol. *See* TLS
transport services 29
troubleshooting
 network views 185
 QTSS 361
trusted binding, policies 340

U

UDP (User Datagram Protocol) 354, 356
UIDs (user IDs) 95–96, 300
Universal Access
 overview 324
 preferences 150, 324
UNIX 305
UNIX and security 27
updating
 software 141, 322
 Software Update service 69–71
 system software 69–72
Upgrading 63
upgrading
 from Mac OS X 63
USB storage devices, disabling 82
user accounts
 administrator 185
 group 187–188, 360, 361
 in directory domains 185
 mobile 314–316
 overview 94–100
 passwords 360
 security 94–??
 settings 176
 See also users
`user filename` keyword 359
user ID. *See* UID
`username` keyword 359
users
 access control 30–32, 176, 212, 288, 357, 360
 auditing 384
 authentication 333–334, 336, 394, 399–401, 402
 automatic actions control 121
 and blog service 294, 295
 categories 274
 certificates 191
 Fast User Switching 312
 home folders 101, 161–??, 162–164, ??–166, 183, 314
 identities 300
 keychain management 110
 mobile 101, 214
 passwords 186
 permissions 152, 186–188, 288, 292
 preferences control 131
 root 86
 unregistered 275
 wireless access 343
 See also clients; computer lists; preferences; user accounts; Workgroup Manager

V

validation, system integrity 376–378
`valid-user` tag 359
video recording devices, disabling 81
view settings 185
virtual memory 174–175
Virtual Private Network. *See* VPN
virus screening 261–269, 270, 271, 273
`visudo` tool 369
VNC (virtual network computing) 40, 58, 62
volumes
 erasing 54
 erasing data 169
 and partitioning 49, 50
 RAID 51, 52
 securing 37
 startup 39, 46
 supported 48
VPN (Virtual Private Network)
 authentication 214
 introduction 213–218
 L2TP settings 35, 215
 and LDAP 218
 PPTP settings 216
 security 214

W

WAN (wide area network) 213
Web-Based Distributed Authoring and Versioning. *See* WebDAV
WebDAV (Web-Based Distributed Authoring and Versioning)
 authentication 289
 configuration 293
 enabling 287
 permissions 288
 realm definitions 288
 starting 287
weblog service 294–295
web modules 287
WebObjects service 298–299
web service 285–292
websites
 access control 288
 accessing 317–319
 folders 288
 security 249, 290
wide area network. *See* WAN

widgets in Dashboard 301, 303
wikis 249
Windows domain
passwords 400
Windows services 283–284, 350
wireless preferences 120–121
workflows 251
Workgroup Manager
access control 32
accounts 185–188
ACL permissions 260
authentication 357
directory domains 179
group account management 187–188
overview 179–180
See also managed preferences
workgroup preferences
See Workgroup Manager
World permission level 274

X

Xgrid 363–368

Z

zones, DNS
security 227
zone transfer, DNS 226